



PATENT ABSTRACTS OF JAPAN

(11) Publication number: **2001143009 A**(43) Date of publication of application: **25.05.01**

(51) Int. Cl. **G06F 19/00**
G06F 12/14
G09C 1/00
G11B 20/10
H04L 9/10

(21) Application number: **2000038875**(22) Date of filing: **16.02.00**

(30) Priority: **17.02.99 JP 11039080**
01.09.99 JP 11247457

(71) Applicant: **NIPPON TELEGR & TELEPH
CORP <NTT>**

(72) Inventor: **TERADA MASAYUKI**
FUJIMURA TAKASHI
KUNO HIROSHI
KAKAN KURAYUKI

(54) **METHOD, SYSTEM AND DEVICE FOR
CIRCULATING ORIGINAL DATA AND
RECORDING MEDIUM WITH ORIGINAL DATA
CIRCULATION PROGRAM RECORDED
THEREON**

processing corresponding to the 2nd information, when
the validity is certified.

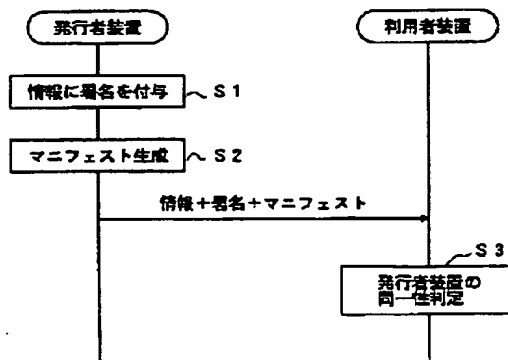
COPYRIGHT: (C)2001,JPO

(57) Abstract

PROBLEM TO BE SOLVED: To provide an original data circulation system for reducing processing loads, such as processing speed and storage capacity.

SOLUTION: This system is provided with an issuer device having a means for generating original information having 1st information, corresponding to the issuer device and 2nd information which corresponds to data and transferring the generated information, a means for verifying the validity of a transfer source device for the original information when the original information is transferred from another device, a user device having a means for storing the original information when the validity is certified, a means for verifying the validity of the original information transfer source information when the original information is transferred from the user device, and a ticket examiner device having a data processing means for executing data

本発明の第1の実施例における原理を説明するための図



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2001-143009

(P2001-143009A)

(43) 公開日 平成13年 5 月25日 (2001. 5. 25)

(51) Int.Cl. ⁷	識別記号	F I	テ-マコード [*] (参考)
G 0 6 F 19/00		G 0 6 F 12/14	3 1 0 Z 5 B 0 1 7
12/14	3 1 0	G 0 9 C 1/00	6 4 0 A 5 B 0 5 5
G 0 9 C 1/00	6 4 0	G 1 1 B 20/10	H 5 D 0 4 4
G 1 1 B 20/10		G 0 6 F 15/30	Z 5 J 1 0 4
H 0 4 L 9/10			L 9 A 0 0 1

審査請求 有 請求項の数71 O L (全 32 頁) 最終頁に続く

(21) 出願番号 特願2000-38875(P2000-38875)

(22) 出願日 平成12年 2 月16日 (2000. 2. 16)

(31) 優先権主張番号 特願平11-39080

(32) 優先日 平成11年 2 月17日 (1999. 2. 17)

(33) 優先権主張国 日本 (J P)

(31) 優先権主張番号 特願平11-247457

(32) 優先日 平成11年 9 月 1 日 (1999. 9. 1)

(33) 優先権主張国 日本 (J P)

(71) 出願人 000004226

日本電信電話株式会社

東京都千代田区大手町二丁目 3 番 1 号

(72) 発明者 寺田 雅之

東京都千代田区大手町二丁目 3 番 1 号 日

本電信電話株式会社内

(72) 発明者 藤村 考

東京都千代田区大手町二丁目 3 番 1 号 日

本電信電話株式会社内

(74) 代理人 100070150

弁理士 伊東 忠彦

最終頁に続く

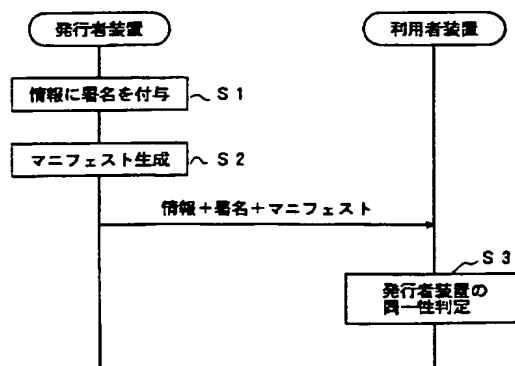
(54) 【発明の名称】 原本データ流通方法、原本データ流通システム及び装置、並びに原本データ流通プログラムを記録した記録媒体

(57) 【要約】

【課題】 処理速度や記憶容量等の処理負荷を低減させる原本データ流通システムを提供する。

【解決手段】 発行者装置に対応する情報を第 1 の情報とデータに対応する第 2 の情報とを有する原本性情報を生成し、転送する手段を有する発行者装置と、他の装置から原本性情報が転送された際に、該原本性情報の転送元装置の正当性を検証する手段と、その正当性が認証された場合に該原本性情報を格納する手段とを有する利用者装置と、利用者装置から原本性情報が転送された際に、該原本性情報の転送元装置の正当性を検証する手段と、その正当性が認証された場合に第 2 の情報に対応するデータに対する処理を行うデータ処理手段とを有する改札者装置とを有する。

本発明の第 1 の実施例における原理を説明するための図



【特許請求の範囲】

【請求項 1】 電子的な情報である原本データの蓄積や流通を行う原本データ流通システムであって、データを発行する発行者装置に対応する第 1 の情報を生成する手段と、該第 1 の情報を転送する手段と、データに対応する第 2 の情報を転送する手段とを有する装置と、受信した第 1 の情報の有効性を判定する手段と、有効な第 1 の情報に対応する発行者装置が正当なものであるかどうかを検証し、正当である場合に前記第 2 の情報に対応するデータを有効と判定する手段とを有する装置とを有することを特徴とする原本データ流通システム。

【請求項 2】 電子的な情報である原本データの蓄積や流通を行う原本データ流通システムにおける原本データ流通方法であって、データを発行する発行者装置に対応する第 1 の情報を生成し、データに対応する第 2 の情報を転送し、前記第 1 の情報を転送し、受信した第 1 の情報の有効性を判定し、有効な第 1 の情報に対応する発行者装置が正当なものであるかどうかを検証し、正当である場合に前記第 2 の情報に対応するデータを有効と判定する原本データ流通方法。

【請求項 3】 価値を有する電子的な情報の蓄積を行うデータ蓄積方法において、電子的な情報の発行者装置による該電子的な情報に対する署名である第 1 の情報を付与するステップと、前記発行者装置により前記第 1 の情報が付与された電子的な情報と対応する第 4 の情報を生成するステップと、電子的な情報利用装置において、前記第 1 の情報と前記第 2 の情報を用いて電子的な情報の発行者装置の同一性を判定し、電子的な情報の複製を防止するステップとを有することを特徴とするデータ蓄積方法。

【請求項 4】 電子的な情報の発行を厳重に管理されたサーバの発行する検証鍵を取得するステップと、前記情報利用装置において、前記検証鍵からセッション情報を生成するステップと、前記セッション情報の正当性を判定するステップとを有する請求項 3 記載のデータ蓄積方法。

【請求項 5】 前記第 2 の情報の格納と、署名者の同一性の判定とを、耐タンパ装置を用いて行うステップを有する請求項 3 記載のデータ蓄積方法。

【請求項 6】 価値を有する電子的な情報の蓄積を行うデータ蓄積システムであって、電子的な情報に第 1 の情報を付与し、該電子的な情報と対応するマニフェストの第 2 の情報を生成する発行者装置と、前記第 1 の情報と前記第 2 の情報を用いて電子的な情報の発行者装置の同一性を判定し、電子的な情報の複製を

防止する利用者装置とを有することを特徴とするデータ蓄積システム。

【請求項 7】 前記利用者装置は、電子的な情報の発行を厳重に管理されたサーバの発行する検証鍵を取得する手段を有し、前記検証鍵からセッション情報を生成する手段と、前記セッション情報の正当性を判定する手段を有する改札装置を更に有する請求項 6 に記載のデータ蓄積システム。

【請求項 8】 前記利用者装置は、前記第 2 の情報を耐タンパ性の装置に格納し、前記発行者装置の同一性を判定する手段を含む請求項 6 記載のデータ蓄積システム。

【請求項 9】 価値を有する電子的な情報の蓄積を行うデータ蓄積システムにおいて該電子的な情報を利用する利用者装置であって、署名が付与された電子的な情報の格納及び抽出を行うための第 1 の格納手段と、前記電子的な情報と 1 対 1 に対応するマニフェストの格納及び抽出を行うための第 2 の格納手段と、該マニフェストが正当であるかどうかを検証する第 1 の認証手段と、該マニフェストが正当であることが前記第 1 の認証手段により検証された時のみ、該マニフェストを前記第 2 の格納手段に格納する第 1 の制御手段とを有することを特徴とする利用者装置。

【請求項 10】 前記第 2 の格納手段及び前記第 1 の認証手段は、耐タンパ性を有する請求項 9 記載の利用者装置。

【請求項 11】 前記第 1 の認証手段は、前記第 1 の格納手段に格納された前記署名が付与された情報の有効性を、該情報と対応するマニフェストが前記第 2 の格納手段に格納されているか否かにより検証し、該マニフェストが該第 2 の格納手段に格納されていたときのみ該情報が有効であるとし、該マニフェストが該第 2 の格納手段に格納されていなかったときには、該情報を無効とする手段を含む請求項 9 記載の利用者装置。

【請求項 12】 情報に署名を付与する署名手段と、マニフェストの署名者が信任対象または、信任対象がさらに信用する署名者に含まれること、及び該信任情報の署名者と、前記電子的な情報の署名者とが同一であることを検証する第 2 の認証手段と、ある電子的な情報に対応するマニフェストを前記第 2 の格納手段から他の格納手段に移動させる際に、該第 2 の格納手段から該マニフェストを抽出し、前記署名手段により該マニフェストに署名を付与し、該第 2 の格納手段から該マニフェストを削除し、該マニフェストの署名者を該電子的な情報の署名者が信用することを前記第 2 の認証手段により検証し、検証に成功した時のみ前記他の格納手段に該マニフェストを格納する第 2 の制御手段と

を含む請求項 9 に記載の利用者装置。

【請求項 13】 前記利用者装置は、システム内で一意性を持つセッション情報を生成するセッション情報生成手段を含み、

該セッション情報は、該利用者装置の検証鍵と連番からなり、該利用者装置に保持されるとともに、マニフェストの送信側に送られ、

該利用者装置は、該送信側から該マニフェストとともに該セッション情報を受信し、該セッション情報の正当性を前記保持したセッション情報を用いて行うことによりマニフェストの複製を防止する請求項 9 に記載の利用者装置。

【請求項 14】 価値を有する電子的な情報の蓄積を行うデータ蓄積システムにおいて該電子的な情報を発行する発行者装置であって、

前記電子的な情報の署名者が信用する署名者を指定する信任対象の 1 つまたは複数の集合からなる信任情報を生成する信任情報生成手段と、

該電子的な情報及び該信任情報に署名を付与する署名手段と、

マニフェストを生成するマニフェスト生成手段と、

該電子的な情報及び該信任情報を利用者装置に送信する手段と、

該利用者装置から、該利用者装置の検証鍵と連番からなるセッション情報を受信する手段と、

該発行者装置の検証鍵と署名関数を用いて前記マニフェストと該セッション情報を含む情報を該利用者装置に送信する手段とを有することを特徴とする発行者装置。

【請求項 15】 価値を有する電子的な情報の蓄積を行うデータ蓄積システムにおいて該電子的な情報の権利を行使する対象である改札者装置であって、

利用者装置から、発行者の署名付きの電子的な情報と信任情報を受信する手段と、

システム内で一意性を持つセッション情報を生成し、該セッション情報を前記利用者装置に送信する手段と、

該利用者装置からマニフェストと該セッション情報を含む情報を受信する手段と、

該マニフェストとセッション情報を含む情報を用いて、セッション情報、マニフェスト及び信任情報が正当であるかどうかを検証する手段を有することを特徴とする改札者装置。

【請求項 16】 価値を有する電子的な情報の蓄積を行うデータ蓄積システムであって、

該データ蓄積システムは、電子的な情報を利用する利用者装置と、電子的な情報を発行する発行者装置と、電子的な情報の権利を行使する対象である改札者装置とを有し、

前記利用者装置は、

署名が付与された電子的な情報の格納及び抽出を行うための第 1 の格納手段と、

前記電子的な情報と 1 対 1 に対応するマニフェストの格納及び抽出を行うための第 2 の格納手段と、

該マニフェストが正当であるかどうかを検証する認証手段と、

該マニフェストが正当であることが前記認証手段により検証された時のみ、該マニフェストを前記第 2 の格納手段に格納する第 1 の制御手段とを有し、

前記発行者装置は、

前記電子的な情報の署名者が信用する署名者を指定する信任対象の 1 つまたは複数の集合からなる信任情報を生成する信任情報生成手段と、

該電子的な情報及び該信任情報に署名を付与する署名手段と、

マニフェストを生成するマニフェスト生成手段と、

該電子的な情報及び該信任情報を利用者装置に送信する手段と、

該利用者装置から、該利用者装置の検証鍵と連番からなるセッション情報を受信する手段と、

該発行者装置の検証鍵と署名関数を用いて前記マニフェストと該セッション情報を含む情報を該利用者装置に送信する手段とを有し、

前記改札者装置は、

利用者装置から、発行者の署名付きの電子的な情報と信任情報を受信する手段と、

システム内で一意性を持つセッション情報を生成し、該セッション情報を前記利用者装置に送信する手段と、

該利用者装置からマニフェストと該セッション情報を含む情報を受信する手段と、

該マニフェストとセッション情報を含む情報を用いて、セッション情報、マニフェスト及び信任情報が正当であるかどうかを検証する手段とを有することを特徴とするデータ蓄積システム。

【請求項 17】 価値を有する電子的な情報の蓄積を行うデータ蓄積システムにおける発行者装置に搭載されるデータ蓄積プログラムを格納した記憶媒体であって、

電子的な情報に署名した第 1 の情報を付与し、該電子的な情報と対応するマニフェストの第 2 の情報を生成して、前記第 1 の情報に付与するプロセスを有することを特徴とするデータ蓄積プログラムを格納した記憶媒体。

【請求項 18】 価値を有する電子的な情報の蓄積を行うデータ蓄積システムにおける利用者装置に搭載されるデータ蓄積プログラムを格納した記憶媒体であって、

前記第 1 の情報と前記第 2 の情報を用いて電子的な情報の発行者装置の同一性を判定し、電子的な情報の複製を防止するプロセスを有することを特徴とするデータ蓄積プログラムを格納した記憶媒体。

【請求項 19】 電子的な情報の発行を厳重に管理されたサーバの発行する検証鍵を取得するプロセスと、

前記検証鍵からセッション情報を生成するプロセスと、

前記セッション情報の正当性を判定するプロセスを含む

請求項18記載のデータ蓄積プログラムを格納した記憶媒体。

【請求項20】 価値を有する電子的な情報の蓄積を行うデータ蓄積システムにおける利用者装置に搭載されるデータ蓄積プログラムを格納した記憶媒体であって、署名が付与された情報を第1の記憶手段に格納すると共に、抽出を行うための第1の格納プロセスと、前記電子的な情報と1対1に対応するマニフェストを第2の記憶手段に格納すると共に、抽出を行うための第2の格納プロセスと、
10 該マニフェストが正当であるかどうかを検証する第1の認証プロセスとを有することを特徴とするデータ蓄積プログラムを格納した記憶媒体。

【請求項21】 前記第1の認証プロセスは、前記第1の記憶手段に格納された前記署名が付与された情報の有効性を、該情報に対応するマニフェストが前記第2の記憶手段に格納されているか否かにより検証し、該マニフェストが該第2の記憶手段に格納されていたときのみ該情報が有効であるとし、該マニフェストが該第2の記憶手段に格納されていなかったときには、該情報を無効とするプロセスを含む請求項20記載のデータ蓄積プログラムを格納した記憶媒体。

【請求項22】 情報に署名を付与するための署名プロセスと、
マニフェストの署名者が信任対象または、信任対象がさらに信用する署名者に含まれること、及び該信任情報の署名者と、前記情報の署名者とが同一であることを検討する第2の認証プロセスとある電子的な情報に対応するマニフェストを移動させる際に、該マニフェストを抽出し、前記署名プロセスにより該マニフェストに署名を付与し、該第2の格納プロセスから該マニフェストを削除し、該マニフェストの署名者を該電子的な情報の署名者が信用することを前記第2の認証プロセスにより検証し、検証に成功した時のみ該マニフェストを移動するプロセスを含む請求項20記載のデータ蓄積プログラムを格納した記憶媒体。

【請求項23】 価値を有する電子的な情報の蓄積を行うデータ蓄積システムにおける発行者装置に搭載されるデータ蓄積プログラムを格納した記憶媒体であって、前記電子的な情報の署名者が信用する署名者を指定する信任対象の1つまたは複数の集合からなる信任情報を生成する信任情報生成プロセスと、
40 該電子的な情報及び該信任情報に署名を付与する署名プロセスと、
マニフェストを生成するマニフェスト生成プロセスと、
該電子的な情報及び該信任情報を利用者装置に送信するプロセスと、
該利用者装置から、該利用者装置の検証鍵と連番からなるセッション情報を受信するプロセスと、
該発行者装置の検証鍵と署名関数を用いて前記マニフェ

ストと該セッション情報を含む情報を該利用者装置に送信するプロセスとを有することを特徴とするデータ蓄積プログラムを格納した記憶媒体。

【請求項24】 価値を有する電子的な情報の蓄積を行うデータ蓄積システムにおける改札装置に搭載されるデータ蓄積プログラムを格納した記憶媒体であって、利用者装置から、発行者の署名付きの電子的な情報と信任情報を受信するプロセスと、
10 システム内で一意性を持つセッション情報を生成し、該セッション情報を前記利用者装置に送信するプロセスと、
該利用者装置からマニフェストと該セッション情報を含む情報を受信するプロセスと、
該マニフェストとセッション情報を含む情報を用いて、セッション情報、マニフェスト及び信任情報が正当であるかどうかを検証するプロセスを有することを特徴とするデータ蓄積プログラムを格納した記憶媒体。

【請求項25】 電子的な情報である原本データの蓄積や流通を行う原本データ流通システムにおける原本データ流通方法であって、
第1の装置が、ある装置に対応する第1の情報と、データもしくは、データに対応する情報である第2の情報と、から構成される原本性情報を転送する転送ステップと、
第2の装置が前記原本性情報の転送元装置を検証し、該転送元装置が認証された場合に該原本性情報を有効であると判別する第1の認証ステップと、
該転送元装置と該原本性情報の第1の情報に対応する装置とが同一であった場合のみ、該第2の装置が該原本性情報を有効であると判別する第2の認証ステップとを有することを特徴とする原本データ流通方法。

【請求項26】 前記第1の装置が秘密鍵を秘匿するステップと、
前記第2の装置が1乃至、複数の秘密鍵に対応する公開鍵の一方関数による出力である自装置のフィンガープリントを保持、または、入手するステップとを更に有し、
前記第1の認証ステップは、
転送元の前記第1の装置が前記フィンガープリントに対応する秘密鍵を保持していることを検証することにより、該転送元の第1の装置を認証するステップを有する請求項25記載の原本データ流通方法。

【請求項27】 前記転送ステップは、
自装置が1乃至複数の第三者によって認証されていることを証明する情報であり、該第三者である認証者に対応する情報である第三者証明を前記第2の装置に転送するステップを有し、
前記原本データ流通方法は、前記第2の装置が1乃至複数の第三者に対応する第三者情報を保持、または、入手するステップを有し、

前記第 1 の認証ステップは、
転送元装置である前記第 1 の装置が前記第三者証明にお
ける認証対象であり、かつ、該第三者証明の認証者のい
ずれかが、保持されている前記第三者情報に対応する第
三者に含まれることを検証することにより、該転送元の
前記第 1 の装置を認証するステップを有する請求項 2 5
記載の原本データ流通方法。

【請求項 2 8】 前記原本データ流通方法は、前記第 2
の装置が前記第 1 の情報と、1乃至複数の第三者に対応
する情報とを対応付ける第三者信頼情報を保持もしく
は、入手するステップを有し、
前記第 1 の認証ステップは、
原本性情報の転送元である前記第 1 の装置が該第三者証
明における認証対象であり、かつ、転送された前記原本
性情報の第 1 の情報から、保持されている前記第三者信
任情報を用いて該第 1 の情報に対応する第三者に対応す
る情報を抽出し、該第三者証明の認証者のいずれかが、
該第三者信頼情報から抽出された第三者に含まれること
を検証することにより、該転送元の第 1 の装置を認証す
るステップを有する請求項 2 7 記載の原本データ流通方
法。

【請求項 2 9】 前記原本データ流通方法は、前記第 2
の装置が前記第 1 の情報と前記第 2 の情報とから、第三
者に対応する情報とを対応づける、前記第三者信頼情報
を保持もしくは、入手するステップを有し、
前記第 1 の認証ステップは、
転送された前記原本性情報の前記第 1 の情報と前記第 2
の情報から、前記第三者信頼情報を用いて該第 1 の情報
と該第 2 の情報の対応する第三者に対応する情報を抽出
し、該第三者証明の認証者のいずれかが、該第三者信
任情報から抽出された第三者に含まれることを検証する
ことにより、該転送元の第 1 の装置を認証するステップ
を有する請求項 2 7 記載の原本データ流通方法。

【請求項 3 0】 前記原本データ流通方法は、
前記第 1 の装置が秘密鍵を秘匿し、前記秘密鍵に対応し
た公開鍵に、自装置を認証する第三者が署名を付与した
公開鍵証明書と該秘密鍵による署名を前記第 2 の装置に
転送するステップと、
前記第 2 の装置が前記公開鍵証明書を検証して署名者の
公開鍵を特定し、1乃至複数のフィガープリントを保持
または、入手するステップとを更に有し、
前記第 1 の認証ステップは、
前記秘密鍵による署名を前記公開鍵証明書が含む公開鍵
により検証し、かつ、該公開鍵証明書の署名者の公開鍵
の一方関数による出力が、保持されている前記フィン
ガープリントに含まれることを検証することにより、転
送元の前記第 1 の装置を認証するステップを有する請求
項 2 5 記載の原本データ流通方法。

【請求項 3 1】 前記原本データ流通方法は、
前記第 2 の装置が、前記第 1 の情報と、1乃至複数の第

1 の装置に対応する情報とを対応付ける利用者信頼情報
を保持もしくは、入手するステップを有し、

前記第 1 の認証ステップは、
転送された前記原本性情報の第 1 の情報から、保持され
ている前記利用者信頼情報を用いて、該第 1 の情報に対
応する第 1 の装置に対応する情報を抽出し、転送元装置
が該利用者信頼情報から抽出された第 1 の装置に含まれ
ることを検証することにより、該転送元の第 1 の装置を
認証するステップを有する請求項 2 5 記載の原本データ
流通方法。

【請求項 3 2】 前記原本データ流通方法は、
前記第 2 の装置が、前記第 1 の情報と前記第 2 の情報か
ら、1乃至複数の前記第 1 の装置に対応する情報とを対
応付ける利用者信頼情報を保持もしくは、入手するステ
ップを有し、
前記第 1 の認証ステップは、
転送された前記原本性情報の第 1 の情報と第 2 の情報と
から、保持されている前記利用者信頼情報を用いて、該
第 1 の情報と該第 2 の情報に対応する第 1 の装置に対
応する情報を抽出し、転送元装置が、該利用者信頼情報
から抽出された第 1 の装置に含まれることを検証するこ
とにより、該転送元の第 1 の装置を認証するステップを
有する請求項 2 5 記載の原本データ流通方法。

【請求項 3 3】 電子的な情報である原本データの蓄積
や流通を行う原本データ流通システムであって、
ある装置に対応する第 1 の情報と、データもしくは、デ
ータに対応する情報である第 2 の情報と、から構成され
る原本性情報を転送する転送手段を有する第 1 の装置
と、

前記原本性情報の転送元装置を特定する特定手段と、該
転送元装置が認証された場合に該原本性情報を有効であ
ると判別する第 1 の認証手段と、該転送元装置と該原本
性情報の第 1 の情報に対応する装置とが同一であった場
合のみ、該原本性情報を有効であると判別する第 2 の認
証手段とを有する第 2 の装置とを有することを特徴とす
る原本データ流通システム。

【請求項 3 4】 前記第 1 の装置は、
秘密鍵を秘匿する手段を更に有し、
前記第 2 の装置は、

1乃至、複数の秘密鍵に対応する公開鍵の一方関数に
よる出力である自装置のフィンガープリントを保持、ま
たは、入手する手段を更に有し、
前記第 2 の装置の前記第 1 の認証手段は、
転送元の前記第 1 の装置が前記フィンガープリントに対
応する秘密鍵を保持していることを検証することによ
り、該転送元の第 1 の装置を認証する請求項 3 3 記載の
原本データ流通システム。

【請求項 3 5】 前記第 1 の装置の前記転送手段は、
自装置が 1乃至複数の第三者によって認証されているこ
とを証明する情報であり、該第三者である認証者に対応

する情報である第三者証明を前記第2の装置に転送する手段を有し、

前記第2の装置は、

1乃至複数の第三者に対応する第三者情報を保持、または、入手する手段を有し、

前記第1の認証手段は、

転送元装置である前記第1の装置が前記第三者証明における認証対象であり、かつ、該第三者証明の認証者のいずれかが、保持されている前記第三者情報に対応する第三者に含まれることを検証することにより、該転送元の

前記第1の装置を認証する請求項3記載の原本データ流通システム。

【請求項36】 前記第2の装置は、前記第1の情報と、1乃至複数の第三者に対応する情報とを対応付ける第三者信頼情報を保持もしくは、入手する手段を有し、

前記第1の認証手段は、

原本性情報の転送元である前記第1の装置が該第三者証明における認証対象であり、かつ、転送された前記原本性情報の第1の情報から、保持されている前記第三者信頼情報を用いて該第1の情報に対応する第三者に対応する情報を抽出し、該第三者証明の認証者のいずれかが、該第三者信頼情報から抽出された第三者に含まれることを検証することにより、該転送元の第1の装置を認証する請求項35記載の原本データ流通システム。

【請求項37】 前記第2の装置は、

前記第1の情報と前記第2の情報とから、第三者に対応する情報とを対応づける、前記第三者信頼情報を保持もしくは、入手する手段を有し、

前記第1の認証手段は、

転送された前記原本性情報の前記第1の情報と前記第2の情報から、前記第三者信頼情報を用いて該第1の情報と該第2の情報の対応する第三者に対応する情報を抽出し、該第三者証明の認証者のいずれかが、該第三者信頼情報から抽出された第三者に含まれることを検証することにより、該転送元の第1の装置を認証する請求項35記載の原本データ流通システム。

【請求項38】 前記第1の装置は、

秘密鍵を秘匿する手段と、

前記秘密鍵に対応した公開鍵に、自装置を認証する第三者が署名を付与した公開鍵証明書と該秘密鍵による署名を前記第2の装置に転送する手段を有し、

前記第2の装置は、

前記公開鍵証明書を検証して署名者の公開鍵を特定する手段と、

1乃至複数のフィガープリントを保持または、入手する手段とを更に有し、

前記第1の認証手段は、

前記秘密鍵による署名を前記公開鍵証明書が含む公開鍵により検証し、かつ、該公開鍵証明書の署名者の公開鍵

の一方関数による出力が、保持されている前記フィガープリントに含まれることを検証することにより、転送元の前記第1の装置を認証する請求項33記載の原本データ流通システム。

【請求項39】 前記第2の装置は、

前記第1の情報と、1乃至複数の第1の装置に対応する情報とを対応付ける利用者信頼情報を保持もしくは、入手する手段を有し、

前記第1の認証手段は、

転送された前記原本性情報の第1の情報から、保持されている前記利用者信頼情報を用いて、該第1の情報に対応する第1の装置に対応する情報を抽出し、転送元装置が該利用者信頼情報から抽出された第1の装置に含まれることを検証することにより、該転送元の第1の装置を認証する請求項33記載の原本データ流通システム。

【請求項40】 前記第2の装置は、

前記第1の情報と前記第2の情報から、1乃至複数の前記第1の装置に対応する情報とを対応付ける利用者信頼情報を保持もしくは、入手する手段を有し、

前記第1の認証手段は、

転送された前記原本性情報の第1の情報と第2の情報とから、保持されている前記利用者信頼情報を用いて、該第1の情報と該第2の情報に対応する第1の装置に対応する情報を抽出し、転送元装置が、該利用者信頼情報から抽出された第1の装置に含まれることを検証することにより、該転送元の第1の装置を認証する請求項33記載の原本データ流通システム。

【請求項41】 電子的な情報である原本データの蓄積や流通を行う原本データ流通システムにおける発行者装置であって、

自装置に対応する情報を第1の情報とし、あるデータもしくは、該データに対応する情報を第2の情報として、原本性情報を生成する原本性情報生成手段と、前記原本性情報を転送する原本性情報転送手段とを有する発行者装置を有することを特徴とする発行者装置。

【請求項42】 秘密鍵を秘匿する手段と、

前記秘密鍵に対応する公開鍵の一方関数による出力である自装置のフィガープリントを前記第1の情報として生成する手段を有する請求項41記載の発行者装置。

【請求項43】 前記原本性情報の前記第2の情報として、データの一方関数による出力を生成する手段を有する請求項41記載の発行者装置。

【請求項44】 前記原本性情報の前記第2の情報として、ネットワーク上の資源の識別子を用いる請求項43記載の発行者装置。

【請求項45】 電子的な情報である原本データの蓄積や流通を行う原本データ流通システムにおける利用者装置であって、

ある装置に対応する第1の情報と、データもしくは、データに対応する情報である第2の情報から構成される原

本性情報を転送する原本性情報転送手段と、
他の装置から原本性情報が転送された際に、該原本性情報の転送元装置を特定する特定手段と、
前記転送元装置が認証された場合、もしくは、該転送元装置と前記原本性情報の第1の情報に対応する装置とが同一であった場合のみ、該原本性情報を有効であると判定する認証手段と、
前記認証手段で前記原本性情報が有効であると判別された場合に、該原本性情報を格納する格納手段とを有することを特徴とする利用者装置。

【請求項46】 自装置から前記原本性情報を転送する際に、該原本性情報を消去する手段を有する請求項45記載の利用者装置。

【請求項47】 電子的な情報である原本データの蓄積や流通を行う原本データ流通システムにおける改札者装置であって、
原本性情報の転送元装置を特定する特定手段と、
前記転送元装置を認証する認証手段と、
前記認証手段において、自装置に転送された前記原本性情報が有効であると判別された場合に、該原本性情報のデータまたは、データに対応する第2の情報に対応するデータに対応する処理を行うデータ処理手段を有することを特徴とする改札者装置。

【請求項48】 発行者装置に対応する情報である発行者情報を保持もしくは、入手する手段を更に有し、
前記データ処理手段は、
前記認証手段において、転送された前記原本性情報が有効であると判別され、かつ、該原本性情報の装置に対応する第1の情報に対応する発行者装置が、保持されている前記発行者情報に対応する発行者装置に含まれる場合に、該原本性情報のデータまたは、データに対応する情報である第2の情報に対応するデータに対する処理を行う請求項47記載の改札者装置。

【請求項49】 電子的な情報である原本データの蓄積や流通を行う原本データ流通システムであって、
発行者装置に対応する情報を第1の情報とデータに対応する第2の情報とを有する原本性情報を生成し、転送する手段を有する発行者装置と、
他の装置から原本性情報が転送された際に、該原本性情報の転送元装置の正当性を検証する手段と、その正当性が認証された場合に該原本性情報を格納する手段とを有する利用者装置と、
利用者装置から原本性情報が転送された際に、該原本性情報の転送元装置の正当性を検証する手段と、その正当性が認証された場合に第2の情報に対応するデータに対する処理を行うデータ処理手段とを有する改札者装置と、
を有することを特徴とする原本データ流通システム。

【請求項50】 電子的な情報である原本データの蓄積や流通を行う原本データ流通システムであって、

自装置に対応する情報を第1の情報とし、あるデータもしくは、該データに対応する情報を第2の情報として、
原本性情報を生成する第1の原本性情報生成手段と、該原本性情報を転送する第1の原本性情報転送手段とを有する発行者装置と、

ある装置に対応する第1の情報と、データもしくは、データに対応する情報である第2の情報から構成される原本性情報を転送する第2の原本性情報転送手段と、他の装置から原本性情報が転送された際に、該原本性情報の転送元装置を特定する第1の特定手段と、該転送元装置が認証された場合、もしくは、該転送元装置と該原本性情報の第1の情報に対応する装置とが同一であった場合のみ、該原本性情報を有効であると判定する第1の認証手段と、該第1の認証手段で該原本性情報が有効であると判別された場合に、該原本性情報を格納する格納手段とを有する利用者装置と、

原本性情報の転送元装置を特定する第2の特定手段と、前記転送元装置を認証する第2の認証手段と、該第2の認証手段において、自装置に転送された該原本性情報が有効であると判別された場合に、該原本性情報のデータまたは、データに対応する第2の情報に対応するデータに対する処理を行うデータ処理手段を有する改札者装置とを有することを特徴とする原本データ流通システム。

【請求項51】 前記改札者装置は更に、
利用者装置から転送された原本性情報を発行者装置に転送する手段を有し、

前記発行者装置は更に、

該原本性情報が該発行者装置の生成したものであるかどうかを検証する手段と、

該原本性情報が正当な流通経路を介して転送されたものであるかどうかを検証する手段と、

前記第2の情報に対応するデータに対する処理が行われたかどうかを検証する手段と、

該データに応じた価値を前記改札者装置に提供する手段と、を有する請求項49に記載の原本性情報データ流通システム。

【請求項52】 前記発行者装置は、
前記データの使用可能回数を度数情報として前記原本性情報に加える手段を更に有し、

前記利用者装置及び前記改札者装置は、それぞれ該度数情報を検証する手段を更に有し、

該利用者装置は、該データを該使用可能回数だけ使用可能である請求項49に記載の原本性情報データ流通システム。

【請求項53】 前記原本データ流通システムにおける装置が原本性情報を転送する際には、前記原本性情報データ流通システム内で一意性を持つセッション情報を共に転送し、

原本性情報を転送する送信側装置は該原本性情報及びセッション情報を保持しておき、

受信側の装置は、該原本性情報を受信すると、該セッション情報を送信側装置に転送し、

該送信側装置は、該原本性情報及び該セッション情報を削除する請求項49に記載の原本データ流通システム。

【請求項54】 前記利用者装置は更に、前記原本性情報を生成する手段を有する請求項49に記載の原本データ流通システム。

【請求項55】 電子的な情報である原本データの蓄積や流通を行う原本データ流通プログラムを格納した記憶媒体であって、

第1の装置に搭載される、

ある装置に対応する第1の情報と、データもしくは、データに対応する情報である第2の情報と、から構成される原本性情報を転送させる転送プロセスと、

第2の装置に搭載される、

前記原本性情報の転送元装置を特定する特定プロセスと、該転送元装置が認証された場合に該原本性情報を有効であると判別する第1の認証プロセスと、該転送元装置と該原本性情報の第1の情報に対応する装置とが同一であった場合のみ、該原本性情報を有効であると判別する第2の認証プロセスとを有することを特徴とする原本データ流通プログラムを格納した記憶媒体。

【請求項56】 前記第1の装置に搭載される、秘密鍵を秘匿するプロセスを更に有し、

前記第2の装置に搭載される、

1乃至、複数の秘密鍵に対応する公開鍵の一方方向関数による出力である自装置のフィンガープリントを保持、または、入手するプロセスを更に有し、

前記第1の認証プロセスは、

転送元の前記第1の装置が前記フィンガープリントに対応する秘密鍵を保持していることを検証することにより、該転送元の第1の装置を認証するプロセスを含む請求項55記載の原本データ流通プログラムを格納した記憶媒体。

【請求項57】 前記第1の装置に搭載されるの前記転送プロセスは、

自装置が1乃至複数の第三者によって認証されていることを証明する情報であり、該第三者である認証者に対応する情報である第三者証明を前記第2の装置に転送するプロセスを有し、

前記第2の装置に搭載される、

1乃至複数の第三者に対応する第三者情報を保持、または、入手するプロセスを有し、

前記第2の装置に搭載される前記第1の認証プロセスは、

転送元装置である前記第1の装置が前記第三者証明における認証対象であり、かつ、該第三者証明の認証者のいずれかが、保持されている前記第三者情報に対応する第三者に含まれることを検証することにより、該転送元の前記第1の装置を認証するプロセスを含む請求項55記

載の原本データ流通プログラムを格納した記憶媒体。

【請求項58】 前記第2の装置に搭載される、

前記第1の情報と、1乃至複数の第三者に対応する情報とを対応付ける第三者信任情報を保持もしくは、入手するプロセスを有し、

前記第1の認証プロセスは、

原本性情報の転送元である前記第1の装置が該第三者証明における認証対象であり、かつ、転送された前記原本性情報の第1の情報から、保持されている前記第三者信任情報を用いて該第1の情報に対応する第三者に対応する情報を抽出し、該第三者証明の認証者のいずれかが、該第三者信任情報から抽出された第三者に含まれることを検証することにより、該転送元の第1の装置を認証するプロセスを含む請求項57記載の原本データ流通プログラムを格納した記憶媒体。

【請求項59】 前記第2の装置に搭載される、

前記第1の情報と前記第2の情報とから、第三者に対応する情報とを対応づける、前記第三者信任情報を保持もしくは、入手するプロセスを有し、

前記第1の認証プロセスは、

転送された前記原本性情報の前記第1の情報と前記第2の情報から、前記第三者信任情報を用いて該第1の情報と該第2の情報の対応する第三者に対応する情報を抽出し、該第三者証明の認証者のいずれかが、該第三者信任情報から抽出された第三者に含まれることを検証することにより、該転送元の第1の装置を認証するプロセスを含む請求項57記載の原本データ流通プログラムを格納した記憶媒体。

【請求項60】 前記第1の装置に搭載される、

秘密鍵を秘匿するプロセスと、

前記秘密鍵に対応した公開鍵に、自装置を認証する第三者が署名を付与した公開鍵証明書と該秘密鍵による署名を前記第2の装置に転送するプロセスを有し、前記第2の装置に搭載される、

前記公開鍵証明書を検証して署名者の公開鍵を特定するプロセスと、

1乃至複数のフィンガープリントを保持または、入手するプロセスとを更に有し、

前記第1の認証プロセスは、

前記秘密鍵による署名を前記公開鍵証明書が含む公開鍵により検証し、かつ、該公開鍵証明書の署名者の公開鍵の一方方向関数による出力が、保持されている前記フィンガープリントに含まれることを検証することにより、転送元の前記第1の装置を認証するプロセスを含む請求項55記載の原本データ流通プログラムを格納した記憶媒体。

【請求項61】 前記第2の装置に搭載される、

前記第1の情報と、1乃至複数の第1の装置に対応する情報とを対応付ける利用者信任情報を保持もしくは、入手するプロセスを有し、

前記第1の認証プロセスは、

転送された前記原本性情報の第1の情報から、保持されている前記利用者信任情報を用いて、該第1の情報に対応する第1の装置に対応する情報を抽出し、転送元装置が該利用者信任情報から抽出された第1の装置に含まれることを検証することにより、該転送元の第1の装置を認証するプロセスを含む請求項5記載の原本データ流通プログラムを格納した記憶媒体。

【請求項62】 前記第2の装置に搭載される、

前記第1の情報と前記第2の情報から、1乃至複数の前記第1の装置に対応する情報を対応付ける利用者信任情報を保持もしくは、入手するプロセスを有し、

前記第1の認証プロセスは、

転送された前記原本性情報の第1の情報と第2の情報とから、保持されている前記利用者信任情報を用いて、該第1の情報と該第2の情報に対応する第1の装置に対応する情報を抽出し、転送元装置が、該利用者信任情報から抽出された第1の装置に含まれることを検証することにより、該転送元の第1の装置を認証するプロセスを含む請求項5記載の原本データ流通プログラムを格納した記憶媒体。

【請求項63】 電子的な情報である原本データの蓄積や流通を行う発行者装置に搭載される原本データ流通プログラムを格納した記憶媒体であって、

前記発行者装置に対応する情報を第1の情報とし、あるデータもしくは、該データに対応する情報を第2の情報として、原本性情報を生成する原本性情報生成プロセスと、

前記原本性情報を転送する原本性情報転送プロセスとを有することを特徴とする原本データ流通プログラムを格納した記憶媒体。

【請求項64】 秘密鍵を秘匿するプロセスと、

前記秘密鍵に対応する公開鍵の一方関数による出力である自装置のフィンガープリントを前記第1の情報として生成するプロセスを有する請求項63記載の原本データ流通プログラムを格納した記憶媒体。

【請求項65】 前記原本性情報の前記第2の情報として、データの一方関数による出力を生成するプロセスを有する請求項63記載の原本データ流通プログラムを格納した記憶媒体。

【請求項66】 前記原本性情報の前記第2の情報として、ネットワーク上の資源の識別子を用いるプロセスを含む請求項65記載の原本データ流通プログラムを格納した記憶媒体。

【請求項67】 電子的な情報である原本データの蓄積や流通を行う利用者装置に搭載される原本データ流通プログラムを格納した記憶媒体であって、

ある装置に対応する第1の情報と、データもしくは、データに対応する情報である第2の情報から構成される原本性情報を転送する原本性情報転送プロセスと、

他の装置から原本性情報が転送された際に、該原本性情報の転送元装置を特定する特定プロセスと、

前記転送元装置が認証された場合、もしくは、該転送元装置と前記原本性情報の第1の情報に対応する装置とが同一であった場合のみ、該原本性情報を有効であると判定する認証プロセスと、

前記認証プロセスで前記原本性情報が有効であると判別された場合に、該原本性情報を格納する格納プロセスとを有することを特徴とする原本データ流通プログラムを格納した記憶媒体。

【請求項68】 前記利用者装置から前記原本性情報を転送する際に、該原本性情報を消去するプロセスを有する請求項67記載の原本データ流通プログラムを格納した記憶媒体。

【請求項69】 電子的な情報である原本データの蓄積や流通を行う改札者装置に搭載される原本データ流通プログラムであって、

原本性情報の転送元装置を特定する特定プロセスと、

前記転送元装置を認証する認証プロセスと、

前記認証プロセスにおいて、自装置に転送された前記原本性情報が有効であると判別された場合に、該原本性情報のデータまたは、データに対応する第2の情報に対応するデータに対応する処理を行うデータ処理プロセスを有することを特徴とする原本データ流通プログラムを格納した記憶媒体。

【請求項70】 発行者装置に対応する情報である発行者情報を保持もしくは、入手するプロセスを更に有し、前記データ処理プロセスは、

前記認証プロセスにおいて、転送された前記原本性情報が有効であると判別され、かつ、該原本性情報の装置に対応する第1の情報に対応する発行者装置が、保持されている前記発行者情報に対応する発行者装置に含まれる場合に、該原本性情報のデータまたは、データに対応する情報である第2の情報に対応するデータに対する処理を行う請求項69記載の原本データ流通プログラムを格納した記憶媒体。

【請求項71】 電子的な情報である原本データの蓄積や流通を行う原本データ流通プログラムを格納した記憶媒体であって、

発行者装置に搭載される、

前記発行者装置に対応する情報を第1の情報とし、あるデータもしくは、該データに対応する情報を第2の情報として、原本性情報を生成する第1の原本性情報生成プロセスと、

前記原本性情報を転送する第1の原本性情報転送プロセスと、

利用者装置に搭載される、

ある装置に対応する第1の情報と、データもしくは、データに対応する情報である第2の情報から構成される原本性情報を転送する第2の原本性情報転送プロセスと、

他の装置から原本性情報が転送された際に、該原本性情報の転送元装置を特定する第1の特定プロセスと、前記転送元装置が認証された場合、もしくは、該転送元装置と該原本性情報の第1の情報に対応する装置とが同一であった場合のみ、該原本性情報を有効であると判定する第1の認証プロセスと、前記第1の認証プロセスで該原本性情報が有効であると判別された場合に、該原本性情報を格納する格納プロセスと、改札者装置に搭載される、原本性情報の転送元装置を特定する第2の特定プロセスと、前記転送元装置を認証する第2の認証プロセスと、前記第2の認証プロセスにおいて、前記改札者装置に転送された該原本性情報が有効であると判別された場合に、該原本性情報のデータまたは、データに対応する第2の情報に対応するデータに対する処理を行うデータ処理プロセスとを有することを特徴とする原本データ流通プログラムを格納した記憶媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、原本データ流通システム及び原本データ流通プログラムを格納した記憶媒体に係り、特に、電子チケットなどの権利を表象するデータやデジタル著作物など、有効な複製数を一定数以下に保つことが必要とされるデータについて、蓄積や配送のための手段を提供するための原本データ流通方法、原本データ流通システム及び装置、並びに原本データ流通プログラムを記録した記録媒体に関する。

【0002】

【従来の技術】権利を表象したデータや著作物などは、配布者などの意図する数を越えて同時に複製が存在することを防止することが求められる。即ち、配布したデータが利用者などにより複製され、それらが多重に利用されることを防ぐ必要がある。

【0003】従来は、以下で示すような技術によりそのような多重利用を防止している。

【0004】第1の方法として、権利を表象するデータについて、権利の提供者などにより、当該データの使用履歴を保持しておき、権利の行使時に、当該データが既に使用されていないかどうかを検証する。もし、既に使用されていれば、当該データが表象する権利の行使を拒否する。

【0005】第2の方法として、データ自身を耐タンバ装置に格納し、当該データを当該耐タンバ装置以外からは参照できないようにする。権利の行使時には、当該データを該耐タンバ装置より抹消する。

【0006】

【発明が解決しようとする課題】しかしながら、上記従来の第1の方法では、耐タンバ装置などの特別な装置を

必要としていないが、データを転々流通させる際に問題が生じる。即ち、当該技術では、行使時の事後検出ししか行えないため、流通過程では、当該データの有効性は判定できないという問題がある。

【0007】従来の第2の方法では、耐タンバ装置を用いることにより、データの唯一性を保証することができる。また、(特願平6-503913)や、(特開平9-511350)などで述べられている方式などを併用し、暗号によって保護された安全な通信路を介して耐タンバ装置を結合し、当該通信路を介してデータの授受を行うことにより、当該データの流通を、複製を事前に防止しながら行うことを可能とする。しかしながら、当該技術は、耐タンバ装置の中にデータを格納する必要があるため、以下の2点が問題となる。

【0008】まず、データの記述そのものを見ることができなくなるため、記述の正当性の検証など、複製に関する有効性以外の検証も全て当該耐タンバ装置に委ねなければならないという制約が生じる。

【0009】また、データの格納部のみならず、データの取扱に必要な処理も全て耐タンバ装置が負わなければならないため、耐タンバ装置に対して記憶容量や処理速度に大きな要求が発生する。特に、現時点で耐タンバ装置として一般的なICカードでは、処理速度や記憶容量に不足が生じる。

【0010】本発明は、上記の点に鑑みなされたもので、データの有効な複製数を一定以下に保つことを保証しつつ、記述の正当性の検証を含む複製に関する有効性以外の検証をすべて耐タンバ装置に委ねることなく、処理速度や記憶容量等の処理負荷を低減させる原本データ流通方法、原本データ流通システム及び装置、並びに原本データ流通プログラムを記録した記録媒体を提供することを目的とする。

【0011】

【課題を解決するための手段】上記の目的を達成させるために、本発明は、次のように構成される。

【0012】本発明は、電子的な情報である原本データの蓄積や流通を行う原本データ流通システムであって、データを発行する発行者装置に対応する第1の情報を生成する手段と、該第1の情報を転送する手段と、データに対応する第2の情報を転送する手段とを有する装置と、受信した第1の情報の有効性を判定する手段と、有効な第1の情報に対応する発行者装置が正当なものであるかどうかを検証し、正当である場合に前記第2の情報に対応するデータを有効と判定する手段とを有する装置とを有する。

【0013】ここでの第1の情報は、例えば、後述するH(PkI)である。また、第2の情報は、例えば、データやデータのハッシュ値である。発行者装置が正当なものであるかどうかは、例えば、上記第2の情報の転送元装置と第1の情報に対応する装置とが同一であるとき、も

しくは該転送元装置が耐タンバ装置であると認証されたときに有効であると判定する。これらの原本性情報の認証処理を耐タンバ装置等が行うことによって、データの取扱いに必要な処理も全て耐タンバ装置等が負わなければならないという従来の問題点を解消することができ、処理速度や記憶容量等の処理負荷を低減させることが可能となる。

【0014】また、本発明は、価値を有する電子的な情報の蓄積を行うデータ蓄積方法であり、電子的な情報の発行者装置による該電子的な情報に対する署名である第3の情報を付与するステップと、前記発行者装置により前記第3の情報が付与された電子的な情報と対応する第4の情報を生成するステップと、電子的な情報利用装置において、前記第3の情報と前記第4の情報を用いて電子的な情報の発行者装置の同一性を判定し、電子的な情報の複製を防止するステップとを有する。

【0015】ここで、第4の情報は、例えば、署名付きデータのハッシュ値として構成されるマニフェストである。マニフェストは原本性情報に対応するものである。これにより、本発明によれば、データ及び当該データに対応する署名を格納し、データと署名付きデータに1対1に対応する情報であるマニフェストを格納し、署名の生成者である署名者を特定し、マニフェストを格納しようとする者が署名者と同一であるかどうかを検証することにより、署名者の意図した数のマニフェストがデータ蓄積システム内に格納される。

【0016】また、本発明は、第4の情報の格納と、署名者の同一性の判定とを、耐タンバ装置を用いて行う。

【0017】これにより、耐タンバ装置を用いることで、データをデータ蓄積システム以外に格納することが可能となる。

【0018】また、本発明は、価値を有する電子的な情報の蓄積を行うデータ蓄積システムであって、電子的な情報に第3の情報を付与し、該電子的な情報と対応するマニフェストの第4の情報を生成する発行者装置と、前記第3の情報と前記第4の情報を用いて電子的な情報の発行者装置の同一性を判定し、電子的な情報の複製を防止する利用者装置とを有する。

【0019】また、本発明は、価値を有する電子的な情報の蓄積を行うデータ蓄積システムにおいて該電子的な情報を利用する利用者装置であって、署名が付与された電子的な情報の格納及び抽出を行うための第1の格納手段と、前記電子的な情報と1対1に対応するマニフェストの格納及び抽出を行うための第2の格納手段と、該マニフェストが正当であるかどうかを検証する第1の認証手段と、該マニフェストが正当であることが前記第1の認証手段により検証された時のみ、該マニフェストを前記第2の格納手段に格納する第1の制御手段とを有する。

【0020】これにより、データに対応するマニフェス

トがデータ蓄積システムに格納されている時のみ、当該データが有効であると区別することにより、マニフェストの数を越えて有効なデータが存在することを防止する。

【0021】また、本発明は、価値を有する電子的な情報の蓄積を行うデータ蓄積システムにおいて該電子的な情報を発行する発行者装置であって、前記電子的な情報の署名者が信用する署名者を指定する信任対象の1つまたは複数の集合からなる信任情報を生成する信任情報生成手段と、該電子的な情報及び該信任情報に署名を付与する署名手段と、マニフェストを生成するマニフェスト生成手段と、該電子的な情報及び該信任情報を利用者装置に送信する手段と、該利用者装置から、該利用者装置の検証鍵と連番からなるセッション情報を受信する手段と、該発行者装置の検証鍵と署名関数を用いて前記マニフェストと該セッション情報を含む情報を該利用者装置に送信する手段とを有する。

【0022】これにより、データの署名者が信用する署名者である信任対象を指定し、マニフェストに、発行者装置を署名者とする署名を付与し、マニフェストの署名者が信任対象または、信任対象がさらに信用する署名者に含まれること、及び信任情報の署名者と、データの署名者とが同一であることを検証する。これにより、当該データの署名者が信用する経路のみを介してマニフェストを移送することが可能となる。さらに、このとき、耐タンバ装置を利用することにより、耐タンバ性が保証される。

【0023】また、本発明は、価値を有する電子的な情報の蓄積を行うデータ蓄積システムにおいて該電子的な情報の権利を行使する対象である改札者装置であって、利用者装置から、発行者の署名付きの電子的な情報と信任情報を受信する手段と、システム内で一意性を持つセッション情報を生成し、該セッション情報を前記利用者装置に送信する手段と、該利用者装置からマニフェストと該セッション情報を含む情報を受信する手段と、該マニフェストとセッション情報を含む情報を用いて、セッション情報、マニフェスト及び信任情報が正当であるかどうかを検証する手段とを有する。

【0024】これにより、本発明では、システム内で一意性を持つセッション情報を生成し、セッション情報を格納することにより、暗号化された通信路を介することなく、1つのマニフェストが複数の格納部に格納されることを防止することが可能となると共に、複数のマニフェストを1つの格納部に並行に転送することが可能となる。

【0025】上記の目的を達成するために、本発明は次のように構成することができる。なお、以下の発明は、後述する第2の実施例において詳細に説明される。

【0026】本発明は、電子的な情報である原本データの蓄積や流通を行う原本データ流通システムにおける原

10

20

30

40

50

本データ流通方法であって、第1の装置が、ある装置に対応する第5の情報と、データもしくは、データに対応する情報である第6の情報と、から構成される原本性情報を転送する転送ステップと、第2の装置が前記原本性情報の転送元装置を検証し、該転送元装置が認証された場合に該原本性情報を有効であると判別する第1の認証ステップと、該転送元装置と該原本性情報の第1の情報に対応する装置とが同一であった場合のみ、該第2の装置が該原本性情報を有効であると判別する第2の認証ステップとを有する。

【0027】また、本発明は、電子的な情報である原本データの蓄積や流通を行う原本データ流通システムであって、ある装置に対応する第5の情報と、データもしくは、データに対応する情報である第6の情報と、から構成される原本性情報を転送する転送手段を有する第1の装置と、前記原本性情報の転送元装置を特定する特定手段と、該転送元装置が認証された場合に該原本性情報を有効であると判別する第1の認証手段と、該転送元装置と該原本性情報の第5の情報に対応する装置とが同一であった場合のみ、該原本性情報を有効であると判別する第2の認証手段とを有する第2の装置とを有する。

【0028】ここで、上記の第5の情報は、例えば、ある装置の検証鍵（公開鍵）のハッシュ値である。また、第6の情報は、例えば、データのハッシュ値である。第5の情報と第6の情報とからなる原本性情報はトークンと称される。上記の発明によれば、第2の認証手段が、転送元装置と前記第5の情報に対応する装置とが同一の場合に原本性情報が有効であると判別するため、データの取扱に必要な処理も全て耐タンバ装置等が負わなければならないという従来の問題点を解消することができ、処理速度や記憶容量等の処理負荷を低減させることが可能となる。また、署名を流通させる必要がないため、更に、処理速度や記憶容量等の処理負荷を低減させることが可能となる。

【0029】また、本発明は、電子的な情報である原本データの蓄積や流通を行う原本データ流通システムにおける発行者装置であって、自装置に対応する情報を第5の情報とし、あるデータもしくは、該データに対応する情報を第6の情報として、原本性情報を生成する原本性情報生成手段と、前記原本性情報を転送する原本性情報転送手段とを有する。

【0030】また、本発明は、電子的な情報である原本データの蓄積や流通を行う原本データ流通システムにおける利用者装置であって、ある装置に対応する第5の情報と、データもしくは、データに対応する情報である第6の情報から構成される原本性情報を転送する原本性情報転送手段と、他の装置から原本性情報が転送された際に、該原本性情報の転送元装置を特定する特定手段と、前記転送元装置が認証された場合、もしくは、該転送元装置と前記原本性情報の第5の情報に対応する装置とが

同一であった場合のみ、該原本性情報を有効であると判定する認証手段と、前記認証手段で前記原本性情報が有効であると判別された場合に、該原本性情報を格納する格納手段とを有する。

【0031】また、本発明は、電子的な情報である原本データの蓄積や流通を行う原本データ流通システムにおける改札者装置であって、原本性情報の転送元装置を特定する特定手段と、前記転送元装置を認証する認証手段と、前記認証手段において、自装置に転送された前記原本性情報が有効であると判別された場合に、該原本性情報のデータまたは、データに対応する第6の情報に対応するデータに対応する処理を行うデータ処理手段を有する。

【0032】また、本発明においては、信用される第三者を特定するフィンガープリントを用いることによって、信用された特定の装置の間だけで原本性情報を流通させることとしている。

【0033】また、本発明は、自装置に対応する情報を第5の情報とし、あるデータもしくは、該データに対応する情報を第6の情報として、原本性情報を生成する第1の原本性情報生成手段と、該原本性情報を転送する第1の原本性情報転送手段とを有する発行者装置と、ある装置に対応する第5の情報と、データもしくは、データに対応する情報である第6の情報から構成される原本性情報を転送する第2の原本性情報転送手段と、他の装置から原本性情報が転送された際に、該原本性情報の転送元装置を特定する第1の特定手段と、該転送元装置が認証された場合、もしくは、該転送元装置と該原本性情報の第5の情報に対応する装置とが同一であった場合のみ、該原本性情報を有効であると判定する第1の認証手段と、該第1の認証手段で該原本性情報が有効であると判別された場合に、該原本性情報を格納する格納手段とを有する利用者装置と、原本性情報の転送元装置を特定する第2の特定手段と、前記転送元装置を認証する第2の認証手段と、該第2の認証手段において、自装置に転送された該原本性情報が有効であると判別された場合に、該原本性情報のデータまたは、データに対応する第6の情報に対応するデータに対する処理を行うデータ処理手段を有する改札者装置とを有する。

【0034】これにより、発行者装置、利用者装置及び改札者装置を有するシステムを構成することにより、これらの装置間において、チケット発行、チケットの譲渡、チケットの消費及びチケットの提示等の各処理を行うことが可能となる。

【0035】

【発明の実施の形態】以下、図面と共に本発明の実施例を説明する。

（第1の実施例）まず、本発明の原本データ流通システムとしてのデータ蓄積システムについて説明する。

【0036】図1は、本発明の原理を説明するための図

である。

【0037】本発明におけるデータ蓄積システムでは、電子的な情報の発行者装置により該電子的な情報に署名した第1の情報に付与し（ステップ1）、発行者装置により電子的な情報と対応するマニフェストの第2の情報を生成して、第1の情報に付与し（ステップ2）、電子的な利用者装置において、第1の情報と第2の情報をを用いて電子的な情報の発行者装置の同一性を判定し（ステップ3）、電子的な情報の複製を防止する。

【0038】図2は、本発明のデータ蓄積システムの全体構成を示す。同図では、権利を表象する電子情報である電子チケットをデータとして発行者が利用者に発行し、チケットを発行された利用者が別の利用者間に譲渡し、チケット譲渡された利用者がチケットを消費する際に、改札者がチケットの有効性を検証する場合を示している。

【0039】同図において、チケットの発行者は、発行者装置1を有し、チケットの発行先となる利用者は利用者装置2を有している。チケットの発行の際には、発行者装置1と利用者装置2の間は、接続装置4を介して通信手段が確立される。この通信手段は、発行の開始から終了までの間のみ確立されていればよい。

【0040】また、チケット譲渡の際には、発行時と同様に利用者装置2間で接続装置4を介して通信手段を確立し、チケットを利用者装置2間で転送する。

【0041】チケットの改札者は、改札者装置3を有している。チケット改札の際には、発行時と同様に、利用者装置2と改札者装置3との間で接続装置4を介して、通信手段を確立し、改札者装置3にチケットを転送する。

【0042】このように、本発明にかかるデータ蓄積システムは、一時的な相互通信手段を提供する接続装置4により接続された、1乃至複数の発行者装置1と、1乃至複数の利用者装置2と、1乃至複数の改札者装置3とから構成されるシステムである。

【0043】ここで、図3から図6を用いて、上記データ蓄積システムを構成する各装置について説明する。以下に、説明で用いる式の意味を示す。

【0044】 $x \parallel y$ とは、 x と y の連接である。

【0045】 H とは、一方向のハッシュ関数であり、 $y=H(x)$ を満たすような x を y から求めることが困難であるという性質を持つ。このようなハッシュ関数として、米RSA社のMD5などが知られている。

【0046】 Sp_k とは、検証関数 V_{Pk} により検証可能な電子署名を生成する署名関数である。

【0047】 V_{Pk} は、検証関数であり、 $V_{Pk}(x \parallel Sp_k(x))=1$ 、 $V_{Pk}(x \parallel \text{other})=0$ ($\text{other} \neq Sp_k(x)$)という性質を持つ。即ち、ある情報 x が署名関数 Sp_k により署名されたものであるかどうかを検証できる性質を持つ。また、電子署名 $Sp_k(x)$ が x に対する Sp_k による正しい署名であるかど

うかを検証できる性質を持つ。

【0048】 Pk は、検証鍵であり、検証器 V に検証鍵 Pk を与えることにより、 V_{Pk} を構成することが可能であるという性質を持つ。署名が付与された検証鍵 $Pk2 \parallel Spk1$ ($Pk2$)を特に、 $Pk1$ による $Pk2$ の鍵証明書と呼ぶ。

【0049】以上で述べたような性質を持つ Sp_k 、 V_{Pk} を実現するような電子署名方式として、日本電信電話のESIGNなどが知られている。

【0050】図3は、本発明の一実施例の発行者装置の構成を示す。

【0051】同図に示す発行者装置1は、制御部11、署名部12、データ生成部13、マニフェスト生成部14、信頼情報生成部15から構成される。

【0052】制御部11は、検証鍵 $Pk1$ を保持し、チケットの流通を安全に行うための制御を行う。ここで、 $Pk1$ は後述する署名部12が備える署名関数 Sp_{k1} に対応する検証鍵である。制御部11による制御の詳細については後述する。

【0053】署名部12は、署名関数 Sp_{k1} を備える。署名関数 Sp_{k1} は、発行者装置1毎にそれぞれ異なり、署名部12により秘匿される。

【0054】データ生成部13は、内部で生成した情報に基づいて、もしくは、外部から与えられた情報に基づいて、データ m を生成する。本発明に係るデータ蓄積システムでは、データ m の記述内容についてなんら制限を持つものではないため、データ m として切符やコンサートチケットなどの一般的なチケットによって扱われる権利を表象する電子情報の他、プログラム、音楽、画像データなどを扱うことが可能である。

【0055】また、外部からデータ m_0 を与え、 $m=H(m_0)$ とするなど、他のデータへの関連として構成することや、他のデータへの関連を含む構成とすることも可能である。このようにすることによって、発行時における耐タンバ装置28への転送データ量を削減することができる。

【0056】マニフェスト生成部14は、一方向のハッシュ関数 h を備え、署名付きデータ $m \parallel Sp_{k1}(m)$ のマニフェスト $c(m, Pk1)=H(m \parallel Sp_{k1}(m))$ を生成する。

【0057】信頼情報生成部15は、信頼情報 $t=(t_I, t_C)$ を生成する。 (t_I, t_C) は、それぞれ以下のように構成される。

【0058】

$t_I = Pk1$

$t_C = (H(PkC_1), H(PkC_2), \dots, H(PkC_n))$

ここで、 $Pk1$ は、制御部11が保持する検証鍵、 PkC_i は発行者が「信用する」第三者（後述）による署名を検証するための検証鍵である。

【0059】図4は、本発明の一実施例の利用者装置の構成を示す。同図に示す利用者装置2は、制御部21、格納部22と、制御部23、認証部24、署名部25、

番号生成部26、格納部27から構成する耐タンバ装置28を有する。各部の機能や内容が改竄されることを（利用者本人からも）防止する。このような耐タンバ装置28として、ＩＣカードや、ネットワーク経由で構成され、第三者により厳重に管理されたサーバなどが利用可能である。

【0060】制御部21は、耐タンバ装置28に封入された制御部23と共に、チケットの流通を安全に行うための制御を行う。制御部21による制御の詳細については後述する。

【0061】格納部22は、利用者が保持する署名付きデータの集合 M_U 及び発行者による署名付きの信任情報の集合 T_U を格納する。これらの集合は、制御部21により更新可能である。

【0062】制御部23は、検証鍵 Pk_U 、 Pk_C 及び鍵証明書 $Spk_U \parallel Spk_C(Pk_U)$ を保持し、制御部21と共に、チケットの流通を安全に行うための制御を行う。ここで Pk_U は署名部25が備える Spk_U に対応する検証鍵であり、 Spk_C は、ＩＣカード製造者もしくは、耐タンバサーバ管理者など、耐タンバ装置28の安全性を保証する第三者により秘匿される署名関数である。即ち、署名関数 Spk_U を含む耐タンバ装置28は、署名関数 Spk_C を保有する第三者により耐タンバ性が保証されている。制御部23による制御の詳細については後述する。また、 Pk_C は、 Spk_C の検証鍵である。

【0063】格納部22は、接続装置4を介して他の利用者装置2の格納部22や改札者装置3の格納部34などと共用することも可能である。この場合、データ m および信任情報(t_1, t_2, t_3)は利用者装置や改札者装置間で共用されることとなるため、以降の実施例においてそれら情報の転送は不要となる。

【0064】認証部24は、検証器 V を備える。

【0065】署名部25は、署名関数 Spk_U を備える。 Spk_U は、利用者装置2毎にそれぞれ異なり、署名部25により秘匿される。

【0066】番号生成部26は、次番号 r_U を保持し、番号の払出しを要求されると、現在の番号 r_U の値を返却すると共に、 r_U をインクリメントする。

【0067】格納部27は、マニフェストの集合 $C_U = \{c_1, c_2, \dots, c_n\}$ 及び番号の集合 $R_U = \{r_1, r_2, \dots, r_m\}$ を格納する。これらの集合は、制御部21により更新可能である。

【0068】図5は、本発明の一実施例の改札者装置の構成を示す。

【0069】同図に示す改札者装置3は、制御部31、認証部32、番号生成部33、及び格納部34から構成される。

【0070】制御部31は、検証鍵 Pk_V を備え、チケットの流通を安全に行うための制御を行う。制御部31による制御の詳細については後述する。

【0071】認証部32は、検証器 V を備える。

【0072】番号生成部33は、次番号 r_V を保持し、番号の払出しを要求されると、 r_V を返却すると共に、 r_V をインクリメントする。

【0073】格納部34は、番号の集合 $R_V = \{r_1, r_2, \dots, r_m\}$ を格納する。これらの集合は、制御部31により更新可能である。

【0074】図6は、本発明の一実施例の接続装置4の構成を示す。

【0075】同図に示す接続装置4は、通信部41を有する。通信部41は、発行者装置1、利用者装置2、改札者装置3間や利用者装置2相互間での一時的もしくは、永続的な通信手段を提供する。ここで、接続装置4としてＩＣカード挿入口を備えたキオスク端末や、ネットワークを介して相互接続された複数のＰＣなどが利用可能である。

【0076】上述したような構成を有する各装置を用いて、電子チケットの流通を安全に行う方式を以下において説明する。

【0077】以下で述べる流通方式における基本的な考え方は、以下のようなものである。

【0078】・チケット本体は、発行者による署名付きのデータ $m \parallel Spk_I(m)$ で表現されるものとする。 m には、発行者がチケットの所有者に与える権利の内容が記述されている、もしくは、権利の内容が記述されているデータへの関連を含むものとする。

【0079】・チケット発行者の署名 Spk_I により、チケットの改竄は防止できる。

【0080】・チケット本体の複製は、特に禁止しない。

【0081】・チケット本体から、そのチケットに対応するマニフェスト $c(m, Pk_I)$ を生成できる。このマニフェストは、事実上チケット本体に1対1に対応する。

【0082】・マニフェストは、発行者が信用できる耐タンバ装置28内の格納部27に格納されることにより、「有効」なものとなる。

【0083】・発行者が信用できる耐タンバ装置とは、発行者が信用する者によって耐タンバ性が保証された装置である。発行者が信用する者は、信任情報 t_1 により規定される。

【0084】・チケットを消費もしくは、譲渡するためには、有効なマニフェストが必要である。

【0085】・有効なマニフェストは、対応するチケットの発行者のみが新規に作成可能である。

【0086】・1つの有効なマニフェストから、複数の有効なマニフェストを作成することを禁止する。即ち、利用者が他者が署名したチケット本体のマニフェストを勝手に作成することを不可能にする。

【0087】以下、(1)チケット発行の場合、(2)チケット譲渡の場合、(3)チケット消費の場合、のそ

れぞれの場合に分けてチケットの流通方式を説明する。
なお、各装置を跨がるそれぞれの通信は、接続装置 4 中の通信部 41 を介するものとする。

【0088】(1) チケット発行の場合：以下は、発行者装置 1 から利用者装置 2 に対する接続装置 4 を介したチケット発行処理の流れである。

【0089】図 7 は、本発明の一実施例のチケット発行処理のシーケンスチャートである。ステップ 101) 制御部 11 は、以下の手順により m 及び $SpkI(m)$ を得て、署名付きデータであるところのチケット $m \parallel SpkI(m)$ の生成を行う。

【0090】(a) データ生成部 13 によりデータ m を生成する。

【0091】(b) 署名部 12 に m を与え、 $SpkI(m)$ を生成する。

【0092】ステップ 102) 制御部 11 は、マニフェスト生成部 14 にチケット $m \parallel SpkI(m)$ を与え、マニフェスト $c(m, PkI)$ を生成する。

【0093】ステップ 103) 制御部 11 は、以下の手順により信頼情報 t 及び署名関数 $SpkI(t)$ を得て、署名付き信頼情報 $t \parallel SpkI(t)$ の生成を行う。

【0094】(a) 信頼情報生成部 15 により、信頼情報 t を生成する。 t の構成は、前述の通りである。

【0095】(b) 署名部 12 に信頼情報 t を与え、署名 $SpkI(t)$ を生成する。

【0096】ステップ 104) 制御部 11 は、制御部 21 にチケット $m \parallel SpkI(m)$ と署名付き信頼情報 $t \parallel SpkI(t)$ を転送する。

【0097】ステップ 101) においてデータ生成部 13 が生成した m が別のデータへの関連、例えば $m = H(m_0)$ などとして構成されている、ないし関連を含む場合は、必要に応じて該関連するデータ (m_0 など) もあわせて転送する。これは、以降で述べるチケット譲渡の場合、チケット消費の場合も同様である。

【0098】ステップ 105) 制御部 21 は、チケット $m \parallel SpkI(m)$ を格納部 22 の M_{ij} に、署名付き信頼情報 $t \parallel SpkI(t)$ を格納部 22 の信頼情報の集合 T_{ij} にそれぞれ追加して格納する。

【0099】 m に関連するデータも転送されてきた場合は、関連を検証し、該検証に失敗した場合は以降の処理を中断し、その旨を通知する。これは、以降で述べるチケット譲渡の場合、チケット消費の場合も同様である。

【0100】ステップ 106) 制御部 21 は、制御部 23 にセッション情報 (s_1, s_2) の生成を依頼する。

【0101】制御部 23 は、以下の手順により、セッション情報 (s_1, s_2) を生成し、制御部 21 に転送する。

【0102】(a) 番号生成部 26 により、番号 ru の払い出しを受ける。

【0103】(b) ru を格納部 27 の番号集合 R_{ij} に追加する。

【0104】(c) (s_1, s_2) = ($H(PkU), ru$) を生成する。ここで、 PkU は、制御部 21 が保持する検証鍵である。

【0105】ステップ 107) 制御部 21 は、制御部 11 にセッション情報 (s_1, s_2) を転送する。

【0106】ステップ 108) 制御部 11 は、署名部 12 が備える $SpkI$ と制御部 11 が保持する検証鍵 PkI を用い、マニフェスト発行形式 $e_i = (e_1, e_2, e_3, e_4, e_5)$ を得る。ここで、 e_i の各要素は以下の値をとる。

【0107】

$e_1 = c(m, PkI)$

$e_2 = s_1$

$e_3 = s_2$

$e_4 = SpkI(c(m, PkI) \parallel s_1 \parallel s_2)$

$e_5 = PkI$

ステップ 109) 制御部 11 は、制御部 21 にマニフェスト発行形式 e_i を転送する。

【0108】ステップ 110) 制御部 21 は、制御部 23 にチケット本体 $m \parallel SpkI(m)$ とマニフェスト発行形式 e_i を転送し、 e_i 内のマニフェストの格納を依頼する。

【0109】ステップ 111) 制御部 23 は、認証部 24 を用い、以下の式で全てが成立することを検証する。検証に失敗した場合、以後の処理を中断し、制御部 21 を介して、制御部 11 に処理の中断の通知を行う。

【0110】

$e_2 = H(PkU)$ (1)

$e_3 \in R_{ij}$ (2)

$V_{e5}(m \parallel SpkI(m)) = 1$ (3)

$V_{e5}(e_1 \parallel e_2 \parallel e_3 \parallel e_4) = 1$ (4)

$e_1 = H(m \parallel SpkI(m))$ (5)

上記の式 (1) 及び式 (2) は、セッション情報の正当性の検証である。この検証により、他の利用者装置 2 宛のマニフェスト発行形式を格納すること、及びマニフェスト発行形式の再利用によってマニフェストを複製すること、などの不正を防止する。式 (3) 及び式 (4)

は、マニフェスト発行形式に対する署名の正当性の検証である。この検証により、チケットの発行者が署名したマニフェスト発行形式に含まれるマニフェスト以外を格納することを防止する。式 (5) はマニフェストとチケット本体の対応の検証である。この検証により、別のチケット本体に対応するマニフェストなど、該チケット本体に対応しないマニフェストの格納を防止する。

【0111】ステップ 112) 制御部 23 は、格納部 27 の番号集合 R_{ij} から $e_3 (= ru)$ を削除する。

【0112】ステップ 113) 制御部 23 は、格納部 27 のマニフェストの集合 C_{ij} に $e_1 (= c(m, PkI))$ を追加する。

【0113】ステップ 114) 制御部 23 は、制御部 21 に e_i を転送し、処理の正常終了を通知する。

【0114】(2) チケット譲渡の場合：以下は、利

用者装置2aから利用者装置2bに対する接続装置4を介したチケット譲渡処理の流れである。

【0115】図8、図9は、本発明の一実施例のチケット譲渡処理のシーケンスチャートである。

【0116】ステップ201) 制御部21aは、格納部22aが保持する署名付きデータの集合 M_{Ua} から譲渡対象となるチケット $m \parallel Sp_{KI}(m)$ を抽出する。

【0117】ステップ202) 制御部21aは、格納部22aが保持する T_{Ua} から $m \parallel Sp_{KI}(m)$ の発行者による署名付き信頼情報 $t \parallel Sp_{KI}(t)$ を抽出する。

【0118】ステップ203) 制御部21aは、制御部21bに $m \parallel Sp_{KI}(m)$ と $t \parallel Sp_{KI}(t)$ を転送する。

【0119】ステップ204) 制御部21bは、 $m \parallel Sp_{KI}(m)$ を格納部22bの署名付きデータの集合 M_{Ub} に、 $t \parallel Sp_{KI}(t)$ を格納部22の信頼情報の集合 T_{Ub} に、それぞれ格納する。

【0120】ステップ205) 制御部21bは、制御部23bにセッション情報(s_1, s_2)の生成を依頼する。制御部23bは、以下の手順により(s_1, s_2)を生成し、制御部21bに転送する。

【0121】(a) 番号生成部26bにより番号 r_{Ub} の払出しを受ける。

【0122】(b) r_{Ub} を格納部27bの番号集合 R_{Ub} に追加する。

【0123】(c) (s_1, s_2)= $(H(Pk_{Ub}), r_{Ub})$ を生成する。ここで、 Pk_{Ub} は、制御部21bが保持する検証鍵である。

【0124】ステップ206) 制御部21bは、制御部21aに(s_1, s_2)を転送する。

【0125】ステップ207) 制御部21aは、制御部23aに(s_1, s_2)と譲渡対象チケットのハッシュ $H(m \parallel Sp_{KI}(m))$ を転送する。

【0126】ステップ208) 制御部23aは、格納部27aに格納されたマニフェスト集合 C_{Ua} について、以下の式が成立することを検証する。検証に失敗した場合、以後の処理を中断し、制御部21aに処理の失敗を通知する。

【0127】
$$H(m \parallel Sp_{KI}(m)) \in C_{Ua} \quad (6)$$

上記の式(6)は、譲渡対象チケットに対応するマニフェスト $c(m, Pk_I) = H(m \parallel Sp_{KI}(m))$ が格納部27aに格納されていることの検証である。

【0128】ステップ209) 制御部23aは、署名部25aが備える Sp_{KUa} と制御部21aが保持する検証鍵 Pk_{Ua} 、 Pk_{Ca} 及び鍵証明書 $Pk_{Ua} \parallel Sp_{KCa}(Pk_{Ua})$ を用い、マニフェスト転送形式 $e_c = (e_1, e_2, e_3, e_4, e_5, e_6, e_7)$ を得る。ここで、 e_c の各要素は、以下の値となる。

【0129】

$e_1 = c(m, Pk_I)$

$e_2 = s_1$

$e_3 = s_2$

$e_4 = Sp_{KUa}(c(m, Pk_I) \parallel s_1 \parallel s_2)$

$e_5 = Pk_{Ua}$

$e_6 = Sp_{KCa}(Pk_{Ua})$

$e_7 = Pk_{Ca}$

ステップ210) 制御部23aは、マニフェスト集合 C_{Ua} から $c(m, Pk_I)$ を削除する。

【0130】ステップ211) 制御部23aは、制御部21aに e_c を転送する。

10 【0131】ステップ212) 制御部21aは、制御部21bに e_c を転送する。制御部21bは、転送された e_c 中の e_1 について、 $e_1 = H(m \parallel Sp_{KI}(m))$ が成立することを検証する。

【0132】ステップ213) 制御部21bは、制御部23bに e_c 、 $t \parallel Sp_{KI}(t)$ 、 $m \parallel Sp_{KI}(m)$ を転送し、 e_c 内のマニフェストの格納を依頼する。

20 【0133】ステップ214) 制御部23bは、認証部24bを用い、以下の式で全てが成立することを検証する。検証に失敗した場合、以後の処理を中断し、制御部21bに処理の中断を通知する。

【0134】

$e_2 = H(Pk_{Ub}) \quad (7)$

$e_3 \in R_{Ub} \quad (8)$

$V_{e5}(e_1 \parallel e_2 \parallel e_3 \parallel e_4, e_5) = 1 \quad (9)$

$V_{e7}(e_5 \parallel e_6) = 1 \quad (10)$

$H(e_7) \in T_C \quad (11)$

$V_{tI}(m \parallel Sp_{KI}(m)) = 1 \quad (12)$

$V_{tI}(t \parallel Sp_{KI}(t)) = 1 \quad (13)$

上記の式(7)及び式(8)は、セッション情報の正当性の検証である。この検証により、他の利用者装置2宛のマニフェスト転送形式を格納すること、及びマニフェスト転送形式の再利用により、マニフェストを複製すること、などの不正を防止する。

【0135】式(9)は、マニフェスト転送形式の署名者を特定するための検証であり、式(10)は、該署名者の鍵証明書の検証であり、式(11)は、当該鍵証明書の署名者が、信頼情報中の信頼対象として発行者により信任されていることの検証である。これらの検証により、発行者が信用する者によって当該マニフェスト転送形式の転送元の耐タンパ性が保証されていることを確認する。

【0136】式(12)及び式(13)は、当該信頼情報に対する署名の正当性の検証である。この検証により、当該信頼情報が当該チケットの署名者により正しく署名されていることを確認する。

【0137】ステップ215) 制御部23bは、格納部27bの番号の集合 R_{Ub} から $e_3 (= r_{Ub})$ を削除する。

【0138】ステップ216) 制御部23bは、格納部27bのマニフェスト集合 C_{Ub} に $e_1 (= c(m, Pk_I))$ を追加する。

【0139】ステップ217) 制御部23bは、制御部21bに処理の正常終了を通知する。

【0140】ステップ218) 制御部21bは、以下の式が成立することを検証する。検証に失敗した場合は、処理の中断を、検証に成功した場合は、処理の正常終了を、制御部21aに通知する。

(3) チケット消費の場合：以下は、利用者装置2から改札者装置3に対する、接続装置4を介したチケット消費処理の流れである。

【0141】図10は、本発明の一実施例のチケット消費のシーケンスチャートである。

【0142】ステップ301) 制御部21は、格納部22が保持する署名付きデータの集合 M_U から消費対象となるチケット $m \parallel \text{SpkI}(m)$ を抽出する。

【0143】ステップ302) 制御部21は、格納部22が保持する署名付き信頼情報の集合 T_U から $m \parallel \text{SpkI}(m)$ の発行者による署名付き信頼情報 $t \parallel \text{SpkI}(t)$ を抽出する。

【0144】ステップ303) 制御部21は、制御部31に $m \parallel \text{SpkI}(m)$ と $t \parallel \text{SpkI}(t)$ を転送する。

【0145】ステップ304) 制御部31は、以下の手順によりセッション情報(s_1, s_2)を生成する。

【0146】(a) 番号生成部33により番号 rv の抽出を受ける。

【0147】(b) rv を格納部34の番号集合 R_V に追加する。

【0148】(c) $(s_1, s_2) = (H(\text{Pkv}), rv)$ を生成する。 Pkv は制御部31が保持する検証鍵である。

【0149】ステップ305) 制御部31は、制御部21にセッション情報(s_1, s_2)を転送する。

【0150】ステップ306) 制御部21は、制御部23に、(s_1, s_2)と消費対象チケットのハッシュ $H(m \parallel \text{SpkI}(m))$ を転送する。

【0151】ステップ307) 制御部23は、格納部27に格納されたマニフェスト集合 C_U について、以下の式が成立することを検証する。検証に失敗した場合は、以後の処理を中断し、制御部21に処理の失敗を通知する。

【0152】 $H(m \parallel \text{SpkI}(m)) \in C_U$ (15)

上記の式(15)は、消費対象チケットに対応するマニフェスト $c(m, \text{Pki}) = H(m \parallel \text{SpkI}(m))$ が格納部27に格納されていることの検証である。

【0153】ステップ308) 制御部23は、署名部25が備える署名関数 SpkU と制御部21が保持する検証鍵 Pku 、 Pkc 及び鍵証明書 $\text{PkU} \parallel \text{SpkC}(\text{PkU})$ を用い、マニフェスト転送形式 $e_c = (e_1, e_2, e_3, e_4, e_5, e_6, e_7)$ を得る。ここで、 e_c の各要素は以下の値をとる。

【0154】 $e_1 = c(m, \text{Pki})$

$e_2 = s_1$

$e_3 = s_2$

$e_4 = \text{SpkU}(c(m, \text{Pki}) \parallel s_1 \parallel s_2)$

$e_5 = \text{Pku}$

$e_6 = \text{SpkC}(\text{PkU})$

$e_7 = \text{Pkc}$

ステップ309) 制御部23は、マニフェスト集合 C_U から $c(m, \text{Pki})$ を削除する。

【0155】ステップ310) 制御部23は、制御部21に e_c を転送する。

【0156】ステップ311) 制御部21は、制御部31に e_c を転送する。

【0157】ステップ312) 制御部31は、認証部32を用い、以下の式の全てが成立することを検証する。検証に失敗した場合は、以後の処理を中断し、制御部21に処理の中断を通知する。

【0158】

$e_2 = H(\text{Pkv})$ (16)

$e_3 \in R_V$ (17)

20 $V_{e_5}(e_1 \parallel e_2 \parallel e_3 \parallel e_4, e_5) = 1$ (18)

$V_{e_7}(e_5 \parallel e_6) = 1$ (19)

$H(e_7) \in t_c$ (20)

$V_{t_I}(m \parallel \text{SpkI}(m)) = 1$ (21)

$V_{t_I}(t \parallel \text{SpkI}(t)) = 1$ (22)

上記の式(16)及び式(17)は、セッション情報の正当性の検証である。この検証により、他の改札者装置3宛のマニフェスト転送形式を格納すること、及び自分宛のマニフェスト転送形式の再利用により、マニフェストを複製すること、などの不正を防止する。

30 【0159】式(18)は、マニフェスト転送形式の署名者を特定するための検証であり、式(19)は、当該署名者の鍵証明書の検証であり、式(20)は、当該鍵証明書の署名者が信頼情報中の信頼対象として発行者により信任されていることの検証である。これらの検証により、発行者が信用する者によって当該マニフェスト転送形式の転送元の耐タンパ性が保証されていることを確認する。

【0160】式(21)及び式(22)は、当該信頼情報に対する署名の正当性の検証である。この検証により、当該信頼情報が当該チケットの署名者により正しく署名されていることを確認する。

【0161】ステップ313) 制御部31は、格納部34の R_V から $e_3 (=rv)$ を削除する。

【0162】ステップ314) 制御部31は、以下の式が成立することを検証する。検証に失敗した場合は、処理の中断を制御部21に通知する。検証に成功した場合は、 m に対応するサービスを消費者に提供する。

【0163】 $e_1 = H(m \parallel \text{SpkI}(m))$ (23)

上記の式(23)は、消費されたチケットに対応するマニフェストが転送されたことの検証である。この検証に

より、有効なマニフェストが併せて転送されたこと、即ち、有効なチケットが消費されたことを確認する。

【0164】また、前述の図2に示す発行者装置1、利用者装置2、改札装置3の各構成要素をプログラムとして構築し、発行者装置、利用者装置、改札装置として利用されるコンピュータに接続されるディスク装置や、フロッピーディスクやCD-ROM等の可搬記憶媒体に格納しておき、本発明を実施する際に、各コンピュータにインストールすることにより容易に本発明を実現できる。

【0165】上述のように、本発明の第1の実施例によれば、データの署名者の意図した数だけマニフェストをデータ蓄積システムのマニフェスト格納部に格納し、当該署名者以外が該マニフェストを新たに格納することを防止する、該マニフェストの数を越えて有効なデータが存在することを防止する、当該署名者が信用する経路のみを介してマニフェストを移送することが可能となる。

【0166】チケットを本発明のデータ蓄積システムのデータとして用いることにより、チケット自体を耐タンパ装置に格納することなしに、チケットの有効な複製数を一定に保つことが可能となる。

【0167】また、プログラムを本発明におけるデータとして用い、当該プログラムの実行ライセンスをマニフェストとして用いることにより、不当に複製された当該プログラムの実行を防止することが可能となる。

【0168】また、音楽データや画像データを本発明におけるデータとして用い、当該データの鑑賞権をマニフェストとして用いることにより、不当に複製された当該データの鑑賞を防止することが可能となる。

【0169】さらに、データを鑑賞する毎に当該データを「消費（実施例における（3））」することにより、利用毎の課金システム（pay per view 課金）などに利用することが可能である。

【0170】（第2の実施例）以下、本発明の第2の実施例について説明する。

【0171】さて、上記の第1の実施例は、原本性を示すデータのみを耐タンパ装置に格納することにより、データの有効な複製数を常に一定以下に保つことを保証しつつ、記述の正当性の検証を含む複製に関する有効性以外の検証を全て耐タンパ装置に委ねることなく、処理速度や記憶容量等の処理負荷を低減させることを特徴としている。この発明は、従来の技術と比較すれば、顕著な効果を奏するが、実用上主に、以下の2点が問題といえる。

【0172】まず、原本性を示すデータの生成時に、データと該データに付与された署名を検証するためにデータ及び該データの署名を耐タンパ装置に転送しなくてはならず、その一方で、ICカードの転送速度は、9600bit/s程度（ISO-7816）と比較的低速であるため、耐タンパ装置としてICカードを用いると、該デ

ータの大きさによっては原本性を示すデータの生成に要する時間を著しく増大させる。

【0173】また、当該技術では、データに対して署名を付与したのに対して原本性を示すデータを生成し、消費の際にも該データ及び該署名を用いて原本性を示すデータの検証が必要となるため、該データのみならず、該署名も共に流通させる必要が生じ、これは、システムに構築のために必要な記憶容量や流通の際の処理時間を増大させる。

10 【0174】第2の実施例では、原本性を示すデータ（トークン）の生成やデータの流通などにおける負荷を低減する原本データ流通システムについて説明する。

【0175】図11は、本発明の第2の実施例の原理構成図である。

【0176】第2の実施例における、電子的な情報である原本データの蓄積や流通を行う原本データ流通システムは、自装置に対応する情報を第1の情報とし、あるデータもしくは、該データに対応する情報を第2の情報として、原本性情報を生成する第1の原本性情報生成手段51と、該原本性情報を転送する第1の原本性情報転送手段52とを有する発行者装置50と、ある装置に対応する第5の情報と、データもしくは、データに対応する情報である第6の情報から構成される原本性情報を転送する第2の原本性情報転送手段61と、他の装置から原本性情報が転送された際に、該原本性情報の転送元装置を特定する第1の特定手段62と、該転送元装置が認証された場合、もしくは、該転送元装置と該原本性情報の第1の情報に対応する装置とが同一であった場合のみ、該原本性情報を有効であると判定する第1の認証手段63と、該第1の認証手段63で該原本性情報が有効であると判別された場合に、該原本性情報を格納する格納手段64とを有する利用者装置60と、原本性情報の転送元装置を特定する第2の特定手段71と、転送元装置を認証する第2の認証手段72と、該第2の認証手段72において、自装置に転送された該原本性情報が有効であると判別された場合に、該原本性情報のデータまたは、データに対応する第2の情報に対応するデータに対する処理を行うデータ処理手段73を有する改札者装置70とを有する。

40 【0177】図12は、本発明の原本データ流通システムにおけるデータ蓄積システムの構成を示す。

【0178】同図において、チケットの発行者は、発行者装置100を有し、チケットの発行先となる利用者は利用者装置200を有している。チケットの発行の際には、発行者装置100と利用者装置200の間は、接続装置400を介して通信手段が確立され、発行者装置100で有効化されたチケットを利用者装置200に転送する。

50 【0179】上記のこれらの装置は、図12（a）、（b）などの構成をとることができる。同図（a）は、

利用者装置200としてICカードを用い、接続装置400としてICカードリーダーを用いる際の代表的な構成を示し、同図(b)は、利用者装置としてICカードなどの耐タンパ装置を装備可能もしくは、安全な場所に保管されたPCを用い、接続装置400としてネットワークを用いる際の代表的な構成を示す。なお、同図(a)、(b)の構成を混在させて用いることも可能である。

【0180】上記の通信手段は、チケットの発行の開始から終了までの間のみ確立させていけばよい。以下、「譲渡」、「消費」、「提示」の際にもこれは同様である。

【0181】チケット譲渡の際には、発行時と同様に利用者装置200間で接続装置400を介して通信手段を確立し、有効なチケットを利用者装置200間で転送する。

【0182】チケットの改札者は、改札者装置300を有している。チケット消費の際には、発行時と同様に利用者装置200と改札者装置300との間で接続装置400を介して通信手段を確立し、利用者装置200から改札者装置300に有効なチケットを転送する。

【0183】チケット提示の際には、2つの利用者装置200の間、もしくは利用者装置200と改札者装置300との間で、接続装置400を介して通信手段を確立し、利用者装置200から他の利用者装置200もしくは、改札者装置300に有効なチケットを所持していることの証明を転送する。

【0184】このように、本発明に係るデータ蓄積システムは、一時的な相互通信手段を提供する1つまたは、複数の接続装置400により接続された、1つまたは、複数の発行者装置100と、1つまたは、複数の利用者装置200と、1つまたは、複数の改札者装置300とから構成されるシステムである。

【0185】以下、図面と共に本発明の実施例を説明する。

【0186】図13から図16を用いて、上記のデータ蓄積システムを構成する各装置について説明する。最初に、以下の説明で用いる式の意味については、ほぼ第1の実施例におけるものと同等である。

【0187】ここでは、検証鍵Pk2及びSpk1によるPk2の電子署名Spk1(Pk2)の組(Pk2, Spk1(Pk2))を特に、Pk1によるPk2の鍵証明書と呼ぶ。また、H(Pk)を特に、Pkのフィンガープリントと呼ぶ。

【0188】図13は、本発明の一実施例の発行者装置の構成を示す。

【0189】図13に示す発行者装置100は、制御部110、署名部120、データ生成部130、トークン生成部140、信頼情報生成部150から構成される。

【0190】制御部110は、検証鍵PkIを保持し、チケットの流通を安全に行うための制御を行う。ここで、

PkIは、後述する署名部120が備える署名関数SpkIに対応する検証鍵であり、そのフィンガープリントH(PkI)は、発行者を特定する識別子として用いられる。制御部110による制御の詳細については、後述する。

【0191】署名部120は、署名関数SpkIを備える。SpkIは、発行者装置100毎にそれぞれ異なり、署名部120により秘匿される。

【0192】データ生成部130は、内部で生成した情報に基づいて、もしくは、外部から与えられた情報に基づいて、データmを生成する。本発明に係るデータ蓄積装置では、データmの記述内容についてなんら制限を持つものではないため、データmとして切符やコンサートチケットなどの一般的チケットによって扱われる権利を表象する電子情報のほか、プログラム、音楽、画像データなどを扱うことが可能である。

【0193】トークン生成部140は、一方向ハッシュ関数Hを備え、データm及び検証鍵PkIよりトークン(c1, c2)=(H(m), H(PkI))

を生成する。ここで、c2は、トークン発行者情報であり、当該トークンの発行者と発行者装置を特定するフィンガープリントである。ここでは、c1にデータmのハッシュ値を用いたが、これにはmを識別する識別子などを用いることも可能である。

【0194】信頼情報生成部150は、信頼情報(t1, t2, t3)を生成する。(t1, t2, t3)は、署名部12を用いて例えば、以下のように構成される。

【0195】

$t_1 = (H(PkA_1), H(PkA_2), \dots, H(PkA_n))$

$t_2 = SpkI(H(PkA_1) \parallel H(PkA_2) \parallel \dots \parallel H(PkA_n))$

$t_3 = PkI$

ここで、H(PkAi)は、発行者が「信用する」第三者(後述)を特定するフィンガープリントである。

【0196】ここで、信頼情報は以下で示す(t'1, t'2, t'3, t'4)のように構成することも可能である。

【0197】

$t'_1 = (H(PkA_1), H(PkA_2), \dots, H(PkA_n))$

$t'_2 = H(m)$

$t'_3 = SpkI(H(PkA_1) \parallel H(PkA_2) \parallel \dots \parallel H(PkA_n) \parallel H(m))$

$t'_4 = PkI$

この場合、H(PkAi)は、発行者が「データmを流通させるにあたって信用するに足る」第三者を特定するフィンガープリントである。

【0198】また、上記信頼情報は、第三者がさらに信頼情報を発行することにより再帰的に構築することも可能である。

【0199】また、さらに、信頼情報を各発行者が生成することをせず、後述する利用者装置の耐タンパ装置の制御部や、改札者装置の制御部が予め固定的に保持しておく形態を採ることも可能である。この場合、署名は必要なく、以下で示す(t''1, t''2)もしくは、t''1のみと

して信頼情報を構成できる。

【0200】

$t''_1 = (H(PkA_1), H(PkA_2), \dots, H(PkA_n))$

$t''_2 = H(m)$

この場合、 $H(PkA_1)$ は、当該制御部（を作成した第三者）が、「（データ m を流通させるにあたって）信用する」第三者を特定するフィンガープリントである。

【0201】以下においては、信頼情報は (t_1, t_2, t_3) と構成されるものとして説明するが、上記のいずれの信頼情報を用いる場合も容易に類推可能である。

【0202】図14は、本発明の一実施例の利用者装置の構成を示す。

【0203】同図に示す利用者装置200は、制御部210、格納部220と、制御部230、認証部240、署名部250、番号生成部260、格納部270から構成される耐タンバ装置280を有する。耐タンバ装置280は、各構成部の機能や内容が改竄されることを（利用者本人からも）防止する。このような耐タンバ装置280として、ICカードや、ネットワーク経由で接続され、第三者により厳重に管理されたサーバなどが利用可能である。

【0204】制御部210は、発行者情報

$I_U = (H(PkI_1), H(PkI_2), \dots, H(PkI_n))$

を備え、耐タンバ装置280に封入された制御部23と共に、チケットの流通を安全に行うための制御を行う。ここで、 I_U は、利用者から「信用された」発行者を示す集合であり、当該利用者により任意の時点で更新可能である。制御部210は、 I_U に含まれる発行者により発行されたトークンのみを有効であると判断する。制御部210による制御の詳細については、後述する。

【0205】また、 I_U をデータごとに発行者情報の集合を管理すること、すなわち $I_U(m_i) = (H(PkI_{i1}), H(PkI_{i2}), \dots, H(PkI_{in}))$ として実現することも可能である。

【0206】格納部220は、利用者が保持するデータの集合 M_U 及び信頼情報の集合 T_U を格納する。これらの集合は、制御部210により更新可能である。

【0207】制御部230は、検証鍵 Pk_U 、 Pk_A 及び鍵証明書 $(Pk_U, Sp_{kA}(Pk_U))$ を保持し、制御部210と共に、チケットの流通を安全に行うための制御を行う。ここで、 Pk_U は、署名部250が備える Sp_{kU} に対応する検証鍵であり、そのフィンガープリント $H(Pk_U)$ は、該利用者装置を特定する識別子として用いる。 Sp_{kA} は、ICカード製造者もしくは耐タンバサーバの管理者など、耐タンバ装置280の安全性を保証する第三者により秘匿される署名関数である。すなわち Sp_{kU} を含む耐タンバ装置280は、 Sp_{kA} を保持する第三者により耐タンバ性を保証されている。制御部230による制御の詳細については後述する。また、 Pk_A は、 Sp_{kA} の検証鍵である。

【0208】認証部240は、検証器 V を備える。

【0209】署名部250は、署名関数 Sp_{kU} を備える。

Sp_{kU} は、利用者装置200毎にそれぞれ異なり、署名部250により秘匿される。

【0210】番号生成部260は、次番号 r_U を保持し、番号の払出しを要求されると当該時点の r_U の値を返却すると共に r_U をインクリメントする。ここで、 r_U は正数である。

【0211】格納部270は、トークンの集合 C_U 及び番号の集合 R_U を格納する。これらの集合は、制御部230により更新可能である。

10 【0212】図15は、本発明の一実施例の改札者装置の構成を示す。

【0213】制御部310は、検証鍵 Pk_E 及び、発行者情報

$I_E = (H(PkI_1), H(PkI_2), \dots, H(PkI_n))$

を備え、チケットの流通を安全に行うための制御を行う。ここで、 I_E は、改札者から「信用された」発行者を示す集合であり、当該改札者により任意の時点で更新可能である。制御部310は、 I_E に含まれる発行者により発行されたトークンのみを正当と判断し、当該トークン

20 を伴うチケットの消費に対してのみサービスを提供する。制御部310による制御の詳細については後述する。

【0214】また、制御部210における I_U と同様に、 I_E をデータごとに発行者情報の集合を管理する、すなわち $I_E(m_i) = (H(PkI_{i1}), H(PkI_{i2}), \dots, H(PkI_{in}))$ として実現することも可能である。

【0215】認証部320は、検証器 V を備える。

【0216】番号生成部330は、次番号 r_E を保持し、番号の払出しを要求されると当該時点の r_E を返却すると共に、 r_E をインクリメントする。ここで、 r_E は正数である。

【0217】格納部340は、番号の集合 R_E を格納する。これらの集合は、制御部310により更新可能である。

【0218】図16は、本発明の一実施例の接続装置の構成を示す。

【0219】同図によれば、接続装置400は、通信部410から構成される。

【0220】通信部410は、発行者装置100、利用者装置200、改札者装置300間や、利用者装置200相互間での、一時的もしくは永続的な通信手段を提供する。ここで、接続装置400として、ICカード挿入口を備えたキオスク端末や、ネットワークを介して相互接続された複数のPC（パーソナルコンピュータ）などが利用可能である。

【0221】上述したような構成を有する各装置100～400を用いて電子チケットの流通を安全に行う方式を以下（1）チケットの発行の場合、（2）チケットの譲渡の場合、（3）チケットの消費の場合、のそれぞれの場合に分けて説明する。なお、各装置を跨がるそれぞ

れの通信は、接続装置400中の通信部410を介するものとする。

【0222】(1) チケット発行の場合：図17は、本発明の一実施例のチケット発行の場合の動作を示すシーケンスチャートである。なお、同図では、発行者装置100と利用者装置200との間に存在する接続装置400は省略してある。

【0223】ステップ1101) 発行者装置100の制御部110は、データ生成部130により、データ m を生成する。当該データ m を権利情報が記述されたチケットであるとする。

【0224】ステップ1102) 発行者装置100の制御部110は、トークン生成部140に m および PkI を与え、トークン $(c_1, c_2) = (H(m), H(PkI))$ を生成する。

【0225】ステップ1103) 制御部110は、信頼情報生成部150により、信頼情報 (t_1, t_2, t_3) を生成する。信頼情報の構成は前述の通りである。

【0226】ステップ1104) 制御部110は、利用者装置200の制御部210に m と (t_1, t_2, t_3) を転送する。

【0227】ステップ1105) 利用者装置200の制御部210は、 m を格納部220の M_U に、 (t_1, t_2, t_3) を格納部220の T_U に、それぞれ追加して格納する。

【0228】ステップ1106) 制御部210は、耐タンバ装置280の制御部230にセッション情報 (s_1, s_2) の生成を依頼し、制御部230は、以下の手順により (s_1, s_2) を生成し、制御部210に転送する。

【0229】(a) 耐タンバ装置280の番号生成部260により番号 r_U の払出しを受ける。

【0230】(b) r_U を格納部270の番号集合 R_U に追加する。

【0231】(c) $(s_1, s_2) = (H(PkU), r_U)$ を生成する。ここで、 PkU は、制御部210が保持する検証鍵である。

【0232】ステップ1107) 制御部210は、発行者装置100の制御部110に (s_1, s_2) を転送する。

【0233】ステップ1108) 発行者装置100の制御部110は、署名部120が備える $SpkI$ と制御部110が保持する検証鍵 PkI を用い、トークン交換形式 $e = (e_1, e_2, e_3, e_4, e_5, e_6, e_7, e_8)$ を得る。ここで、 e の各要素は、以下の値となる。また、チケット発行の際においては e_7 及び e_8 はダミーであり、それぞれ任意の値を持たせてよい。

【0234】

$e_1 = c_1$

$e_2 = c_2$

$e_3 = s_1$

$e_4 = s_2$

$e_5 = SpkI(c_1 \parallel c_2 \parallel c_3 \parallel c_4)$

$e_6 = PkI$

$e_7 = any$ (任意)

$e_8 = any$ (任意)

ステップ1109) 発行者装置100の制御部110は、利用者装置200の制御部210に e を転送する。

【0235】ステップ1110) 利用者装置200の制御部210は、耐タンバ装置280の制御部230に e を転送し、 e 内のトークンの格納を依頼する。

【0236】ステップ1111) 耐タンバ装置280の制御部230は、認証部240を用いて、以下の式の全てが成立することを検証する。検証に失敗した場合、以後の処理を中断し、制御部210を介して、発行者装置100の制御部110に処理を中断を通知する。

【0237】

$e_3 = H(PkU)$ (1)

$e_4 \in R_U$ (2)

$V_{e6}(e_1 \parallel e_2 \parallel e_3 \parallel e_4, e_5) = 1$ (3)

$e_2 = H(e_6)$ (4)

上記の式(1)及び式(2)は、セッション情報の正当性の検証である。この検証により、当該利用者装置2以外に宛られたトークン交換形式を格納すること、及びトークン交換形式の再利用によってトークンを複製すること、などによる不正を防止する。

【0238】式(3)は、トークン交換形式に対する署名の正当性の検証であり、この検証によりトークン交換形式の改竄を防止する。

【0239】また、式(4)は、トークン発行者情報の正当性の検証であり、当該トークンの署名者以外が発行者となるトークンを格納することを防止する。

【0240】ステップ1112) 利用者装置200の耐タンバ装置280の制御部230は、格納部270の R_U から $e_4 (= r_U)$ を削除する。

【0241】ステップ1113) 耐タンバ装置280の制御部230は、格納部270の C_U に (e_1, e_2) を追加する。

【0242】ステップ1114) 耐タンバ装置280の制御部230は、制御部210に (e_1, e_2) を転送し、処理の正常終了を通知する。

【0243】ステップ1115) 制御部210は、以下の式が成立することを検証する。検証に失敗した場合は、処理の中断を、検証に成功した場合は処理の正常終了を、発行者装置100の制御部110に通知する。

【0244】

$e_1 = H(m)$ (5)

$e_2 \in I_U$ (6)

式(5)及び式(6)は、転送されたトークンが、対象とするチケットに対応し、正当な発行者によって発行されたものであることの検証である。この検証により、発行されたチケットが有効であることを確認する。

【0245】(2) チケット譲渡の場合：以下は、利

用者装置200aから利用者装置200bに対する、接続装置400を介したチケット譲渡処理の流れである。

【0246】図18、図19は、本発明の一実施例のチケット譲渡の場合の動作を示すシーケンスチャートである。なお、同図において2つの利用者装置200a、200bの間に存在する接続装置400は省略してある。また、利用者装置200aの各構成要素の各々にはaを付し、利用者装置200bの各構成要素の各々にはbを付す。

【0247】ステップ2201) 利用者装置200aの制御部210aは、格納部220aが保持する M_{Ua} から譲渡対象となるチケット m を抽出する。

【0248】ステップ2202) 利用者装置200aの制御部210aは、格納部220aが保持する T_{Ua} から m の発行者による信頼情報(t_1, t_2, t_3)を抽出する。

【0249】ステップ2203) 制御部210aは、利用者装置200bの制御部210bに m と(t_1, t_2, t_3)を転送する。

【0250】ステップ2204) 利用者装置200bの制御部210bは、 m を格納部220bの M_{Ub} に、(t_1, t_2, t_3)を格納部220bの T_{Ub} にそれぞれ格納する。

【0251】ステップ2205) 制御部210bは、耐タンバ装置280bの制御部230bにセッション情報(s_1, s_2)の生成を依頼する。制御部230bは、以下の手順により(s_1, s_2)を生成し、制御部210bに転送する。

【0252】(a) 耐タンバ装置280bの番号生成部260bにより番号 r_{Ub} の払出しを受ける。

【0253】(b) r_{Ub} を耐タンバ装置280bの格納部270bの番号集合 R_{Ub} に追加する。

【0254】(c) (s_1, s_2)= $(H(Pk_{Ub}), r_{Ub})$ を生成する。ここで、 Pk_{Ub} は、制御部210bが保持する検証鍵である。

【0255】ステップ2206) 制御部210bは、利用者装置200の制御部210aに(s_1, s_2)を転送する。また、 T_{Ub} をあわせて転送するようにしてもよい。発行者情報の事前通知を行うことによって、式(16)や式(26)の検証に失敗するようなトークン交換形式を生成、送信することを未然に防止できる。

【0256】ステップ2207) 利用者装置200aの制御部210aは、耐タンバ装置280aの制御部230aに(s_1, s_2)と譲渡対象チケットのハッシュ $H(m)$ を転送する。

【0257】ステップ2208) 利用者装置200aの耐タンバ装置280aの制御部230aは、格納部270aに格納された C_{Ua} について、以下の式が成立することを検証する。検証に失敗した場合、以後の処理を中断し、制御部210aに処理の失敗を通知する。

【0258】 $\exists c_2((H(m), c_2) \in C_{Ua}), \quad c_2 \in I_{Ub} \quad (7)$

式(7)は、譲渡対象チケット m に対応するトークン($H(m), c_2$)が耐タンバ装置280の格納部270aに格納されていることの検証である。

【0259】ステップ2209) 耐タンバ装置280aの制御部230aは、署名部250aが備える Spk_{Ua} と利用者装置200aの制御部210aが保持する検証鍵 Pk_{Ua} 、 Pk_{Aa} 及び、鍵証明書($Pk_{Ua}, Spk_{Aa}(Pk_{Ua})$)を用い、トークン交換形式 $e=(e_1, e_2, e_3, e_4, e_5, e_6, e_7, e_8)$ を得る。ここで、 e の各要素は以下の値をとる。

【0260】
$$\begin{aligned} e_1 &= H(m) \\ e_2 &= c_2 \\ e_3 &= s_1 \\ e_4 &= s_2 \\ e_5 &= Spk_{Ua}(H(m) \parallel c_2 \parallel s_1 \parallel s_2) \\ e_6 &= Pk_{Ua} \\ e_7 &= Spk_{Aa}(Pk_{Ua}) \\ e_8 &= Pk_{Aa} \end{aligned}$$

ステップ2210) 利用者装置200aの耐タンバ装置280aの制御装置230aは、 s_2 が正であるなら、 C_{Ua} から($H(m), c_2$)を削除する。

【0261】ステップ2211) 耐タンバ装置280aの制御部230aは、制御部210aに e を転送する。

【0262】ステップ2212) 制御部210aは、利用者装置200bの制御部210bに e を転送する。

【0263】ステップ2213) 制御部210bは、耐タンバ装置280bの制御部230bに e と対応する信頼情報 t を転送し、 e 内のトークンの格納を依頼する。

【0264】ステップ2214) 制御部230bは、認証部240bを用いて、以下の式の全てが成立することを検証する。検証に失敗した場合、以後の処理を中断し、制御部210bに処理の中断を通知する。

【0265】
$$\begin{aligned} e_3 &= H(Pk_{Ub}) & (8) \\ e_4 &\in R_{Ub} & (9) \\ \forall e_6(e_1 \parallel e_2 \parallel e_3 \parallel e_4, e_5) &= 1 & (10) \\ \forall e_8(e_6, e_7) &= 1 & (11) \\ H(e_8) &\in t_1 & (12) \\ \forall t_3(t_1, t_2) &= 1 & (13) \\ e_2 &= H(t_3) & (14) \end{aligned}$$

式(8)及び式(9)は、セッション情報の正当性の検証である。この検証により、当該利用者装置200b以外に宛られたトークン交換形式を格納すること、及びトークン交換形式の再利用によってトークンを複製すること、などによる不正を防止する。

【0266】式(10)は、トークン交換形式に対する署名の正当性の検証であり、この検証によりトークン交換形式の改竄を防止する。

【0267】式(11)は、当該署名者の鍵証明書の検証である。また、式(12)は、該鍵証明書の署名者が、信任情報中の信任対象に含まれることの検証であり、式(13)は、該信任情報の正当性の検証であり、式(14)は、該信任情報の署名者が該トークンの発行者と等しいかどうかの検証である。これらの検証により、該発行者が信用する者によって、該トークン交換形式転送元の耐タンバ性が保証されていることを確認する。

【0268】ステップ2215) 利用者装置200の耐タンバ装置280bの制御部230bは、格納部270bの R_{Ub} から $e_4 (=r_{Ub})$ を削除する。

【0269】ステップ2216) 制御部230bは、格納部270bの C_{Ub} に(e_1, e_2)を追加する。

【0270】ステップ2217) 制御部230bは、制御部210bに処理の正常終了を通知する。

【0271】ステップ2218) 制御部210bは、以下の式が成立することを検証する。検証に失敗した場合は処理の中断を、検証に成功した場合は処理の正常終了を、制御部210aに通知する。

【0272】

$$e_1 = H(m) \quad (15)$$

$$e_2 \in I_{Ub} \quad (16)$$

式(15)及び式(16)は、転送されたトークンが、対象となるチケットに対応し、正当な発行者によって発行されたものであることの検証である。この検証により、譲渡されたチケットが有効であることを確認する。

【0273】制御部210bにおいて発行者情報がデータごとに管理されている場合は、式(16)は $e_2 \in I_{Ub}(m)$ となる。

【0274】(3) チケット消費の場合：以下は、利用者装置200から改札者装置300に対する接続装置400を介したチケット消費処理の流れである。

【0275】図20は、本発明の一実施例のチケット消費の場合の動作を示すシーケンスチャートである。

【0276】なお、同図において、利用者装置200と改札者装置300間に存在する接続装置400は省略する。

【0277】ステップ3301) 利用者装置200の制御部210は、格納部220が保持する M_U から譲渡対象となるチケット m を抽出する。

【0278】ステップ3302) 制御部210は、格納部220が保持する T_U から m の発行者による信任情報(t_1, t_2, t_3)を抽出する。

【0279】ステップ3303) 制御部210は、改札者装置300の制御部310に m と(t_1, t_2, t_3)を転送する。

【0280】ステップ3304) 制御部310は、以下の手順により(s_1, s_2)を生成する。

【0281】(a) 番号生成部330により番号 r_E の

払出しを受ける。

【0282】(b) r_E を格納部340の番号集合 R_E に追加する。

【0283】(c) (s_1, s_2)= $(H(PkE), r_E)$ を生成する。ここで、 PkE は制御部310が保持する検証鍵である。

【0284】ステップ3305) 制御部310は、利用者装置200の制御部210に(s_1, s_2)を転送する。

【0285】ステップ3306) 制御部210は、耐タンバ装置280の制御部230に(s_1, s_2)と消費対象チケットのハッシュ $H(m)$ を転送する。

【0286】ステップ3307) 耐タンバ装置280の制御部230は、格納部270に格納された C_U について、以下の式が成立することを検証する。検証に失敗した場合、以後の処理を中断し、制御部210に処理の失敗を通知する。

$$[0287] \exists c_2 ((H(m), c_2) \in C_U) \quad (17)$$

式(17)は、譲渡対象チケット m に対応するトークン($H(m), c_2$)が耐タンバ装置280の格納部270に格納されていることの検証である。

【0288】ステップ3308) 耐タンバ装置280の制御部230は、署名部250が備える Spk_U と利用者装置200の制御部210が保持する検証鍵 Pk_U 、 Pk_A 及び、鍵証明書($Pk_U, Spk_A(Pk_U)$)を用い、トークン交換形式 $e=(e_1, e_2, e_3, e_4, e_5, e_6, e_7, e_8)$ を得る。ここで、 e の各要素は以下の値を採る。

【0289】

$$e_1 = H(m)$$

$$e_2 = c_2$$

$$e_3 = s_1$$

$$e_4 = s_2$$

$$e_5 = Spk_U(H(m) \parallel c_2 \parallel s_1 \parallel s_2)$$

$$e_6 = Pk_U$$

$$e_7 = Spk_A(Pk_U)$$

$$e_8 = Pk_A$$

ステップ3309) 耐タンバ装置280の制御部230は、 s_2 が正であるなら、 C_U から($H(m), c_2$)を削除する。

【0290】ステップ3310) 耐タンバ装置280の制御部230は、制御部210に e を転送する。

【0291】ステップ3311) 制御部210は、改札者装置300の制御部310に e を転送する。

【0292】ステップ3312) 認証部320を用い、以下の式の全てが成立することを検証する。検証に失敗した場合、以後の処理を中断し、利用者装置200の制御部210の処理の中断を通知する。

【0293】

$$e_3 = H(PkE) \quad (18)$$

$$e_4 \in R_E \quad (19)$$

$$V_{e6}(e_1 \parallel e_2 \parallel e_3 \parallel e_4, e_5) = 1 \quad (20)$$

$$V_{e8}(e_6, e_7) = 1 \quad (21)$$

$$H(e_8) \in t_1 \quad (22)$$

$$V_{t3}(t_1, t_2) = 1 \quad (23)$$

$$e_2 = H(t_3) \quad (24)$$

式(18)及び式(19)は、セッション情報の正当性の検証である。この検証により、当該改札者装置300以外に宛られたトークン交換形式の利用や、トークン交換形式の再利用などによる不正を防止する。

【0294】式(20)は、トークン交換形式に対する署名の正当性の検証であり、この検証により、トークン交換形式の改竄を防止する。

【0295】式(21)は、当該署名者の鍵証明書を検証である。また、式(22)は、該鍵証明書の署名者が、信任情報中の信任対象に含まれることの検証であり、式(23)は、該信任情報の正当性の検証であり、式(24)は、該信任情報の署名者が該トークンの発行者と等しいかどうかの検証である。これらの検証により、該発行者が信用する者によって、該トークン交換形式転送元の耐タンバ性が保証されていることを確認する。

【0296】ステップ3313) 改札者装置300の制御部310は、格納部340の R_E から $e_4 (=r_E)$ を削除する。

【0297】ステップ3314) 制御部310は、以下の式が成立することを検証する。検証に失敗した場合は、処理に中断を利用者装置200の制御部210に通知する。検証に成功した場合は、 m に対応するサービスをチケットの消費者に提供する。

【0298】

$$e_1 = H(m) \quad (25)$$

$$e_2 \in I_E \quad (26)$$

式(25)及び式(26)は、転送されたトークンが対象となるチケットに対応し、正当な発行者によって発行されたものであることの検証である。この検証により、消費されたチケットが有効であることを確認する。

【0299】制御部31において発行者情報がデータごとに管理されている場合は、式(26)は $e_2 \in I_E(m)$ となる。

【0300】(4) チケット提示の場合：チケット提示は、(3)チケット消費の場合の処理において、以下の変更を加えることにより可能になる。

【0301】・ステップ3304の(c)において、 $(s_1, s_2) = (H(Pk_E), -r_E)$ を生成する。

【0302】・ステップ3312において、式(19)を $-e_4 \in R_E$ とする。

【0303】以上の変更により、 s_2 が負数となるため、ステップ3309において、 C_U からの削除は行われな

トの検札が可能となる。

【0304】なお、以上のそれぞれの場合(1)～

(4)の説明において、転送されたトークン交換形式は、明示的に保存しなかった。しかしながら、該トークン交換形式の格納部220などに保存しておき、該トークン交換形式及び m の受信の際に共に受信したトークン交換形式の履歴を m の送信の際に共に送信することにより、耐タンバ装置28が破られるなどして不正行為(二重使用)が発見された場合に、不正が行われた装置を特定することが可能となる。

【0305】(5)チケットの還流

次に、改札者が消費、提示を受けたチケットを発行者に還流し、対価を発行者が改札者に支払う場合について説明する。このようにすることによって、改札や検札を行なった改札者に対して、二重請求を防ぎつつ手数料などの対価を提供することが可能になる。

【0306】発行者装置100は、トークン交換形式 e を格納する手段(格納部160)と、還流されるチケットに対応するデータ m および信任情報(t_1, t_2, t_3)を保持または入手する手段をさらに有するものとする。

【0307】以下は、改札者装置300が消費または提示を受けたチケットを発行者装置100に還流するチケット還流処理の流れである。

【0308】ステップ5501) 改札者装置300は、消費または提示を受けたチケットに対応するトークン交換形式 e を発行者装置100に転送する。

【0309】ステップ5502) 発行者装置100の制御部110は、 e に含まれる e_2 について、 $e_2 = H(Pk_I)$ であることを検証する。検証に失敗した場合、その旨を通知するとともに以後の処理を中断する。これは、 e が自身が発行したチケットに対応するものであるかどうかの検証である。

【0310】ステップ5503) 制御部110は、 e について式(20-22)が成立することを検証する。ただし、信任情報(t_1, t_2, t_3)が信頼できない経路(改札者など)から入手された場合、式(23、24)もあわせて検証する。ただし、式(24)の検証では、 t_3 の代わりに Pk_I を用いる。検証に失敗した場合、その旨を通知するとともに以後の処理を中断する。これは、 e が正当な流通経路を介して流通されたことの検証である。

【0311】ステップ5504) 制御部110は、 e_4 が正である場合、 e に含まれる e_3 について、 e_3 が t_1 によって信任された第3者によって、耐タンバ性を保証されていないことを検証する。これは、 e により有効なトークンが格納されていない(消費により正しく権利が消滅した)ことの検証である。

【0312】ステップ5505) 制御部110は、 e を格納部160に格納する。もし、すでに e が格納部160に格納済であった場合、その旨を通知するとともに以後の処理を中断する。

【0313】ステップ5506) 発行者は、還流されたチケットに応じた対価を改札者に提供する。

【0314】(6) 回数券

次に、トークンおよびトークン交換形式に、度数ないし個数に相当する数値情報を追加し、対応するチケットの「枚数」とし、回数券を実現する例について説明する。

【0315】これにより、同一内容、同一発行者のチケットが複数発行されても正しく扱えるようにするとともに、複数の同一トークンを効率的に送信できるようになる。

【0316】具体的には、上述した実施例における以下の変更により上記の回数券は実現される。

【0317】・トークンに度数情報 c_3 を追加する。

【0318】・トークン交換形式に度数情報 e_n を追加する。

【0319】・チケット発行において、トークン生成時(S1102)に発行するチケット枚数を n として指定する。

【0320】・チケット譲渡/消費において、(S2207, S3306)の際に譲渡/消費するチケット枚数を n として指定する。

【0321】・チケット譲渡/消費において、トークン保持の検証時(S2208-S3307)に、度数が充分にあることを検証する。すなわち、 $c_1 = H(m) \cap c_3 \geq n$ が成立する(c_1, c_2, c_3)が C_U に含まれることを検証する。

【0322】・全処理において、トークン交換形式生成時(S1108, S2209, S3308)に、 $e_n = n$ を追加するとともに、 e_5 の署名対象に n を追加して連接する($c_1 \parallel c_2 \parallel s_1 \parallel s_2 \parallel n$ となる。)

・チケット譲渡/消費において、トークン削除時(S2210, S3309: s_2 が正の場合)に、 $c_3 = n$ の場合にのみ($H(m), c_2, c_3$)を C_U から削除し、 $c_3 > n$ の場合は C_U の($H(m), c_2, c_3$)を($H(m), c_2, c_3 - n$)に更新する。

【0323】・全処理において、トークン交換形式検証時(S1111, S2214, S3312)の e_5 による署名検証(式(3), 式(10), 式(20))の検証対象に e_n を追加して連接する($e_1 \parallel e_2 \parallel e_3 \parallel e_4 \parallel e_n$ となる)。

【0324】・チケット発行/譲渡において、トークン格納時(S1113, S2216)に $e_1 = c_1, e_2 = c_2$ が共に成立するトークン(c_1, c_2, c_3)が C_U にすでに存在する場合、 C_U 中の該トークン(c_1, c_2, c_3)を($c_1, c_2, c_3 + e_n$)に更新する。

【0325】・チケット消費/還流において、サービスや対価の提供はさらに e_n にも応じて行なう。

【0326】(7) 再送制御

次に、転送路の不意の切断など、異常が発生した後にトークンの再送を(複製を防ぎつつ)可能にするための処理について説明する。

【0327】具体的には、各手順に、以下の処理を追加する。

【0328】・制御部110、230は、トークン交換

形式の生成(S1108, S2209-S3308)の際に、生成したトークン交換形式 e を保持する。

【0329】・制御部210、310は、受領通知(S1115, S2218における正常終了, S3314におけるサービスの提供)の際に、(チケット送り側の)制御部110、210に(s_1, s_2)を通知する。

【0330】・制御部110、210は、上記受領通知を受けたら、(s_1, s_2)に対応するトークン交換形式を消去する。

10 【0331】また、再送の際は、各手順において以下の変更を行なう。

【0332】・セッション情報生成(S1106, S2205, S3304)の際に、(新規にセッション情報を生成するのではなく)格納部220、340に格納されているセッション情報(s_1, s_2)を用いる。

20 【0333】・トークン交換形式生成に関連する処理(S1108, S2208-2210, S3307-S3309)において、制御部110、210が($e_3 = s_1$) \cap ($e_4 = s_2$)が成立する e を保持している場合、これらの処理により e を生成せず、保持している e を用いて以後の処理を行なう。

【0334】(8) 発行のバリエーション

チケット発行とは、論理的にはチケット(トークン)生成+チケット譲渡と考えることができるため、たとえば以下のような手順によりチケット譲渡処理を用いてチケットの発行を行なうことが可能である。ただし、チケット発行よりもチケット譲渡のほうが検証処理が多いため、両手順とも本来のチケット発行と比較して処理量は増大する。

【0335】(8-1) 自己証明書の利用

30 下記のようにすることにより、制御部230によるトークン交換形式の検証は、チケット発行(S1111)とチケット譲渡(S2214)とで異なる。これを(S2214における検証で)一本化し、制御部230の実装コストを軽減する。

【0336】制御部110は、自己による鍵証明書($Pk_I, Spk_I(Pk_I)$)を保持する。以下、チケット発行の手順において、以下の変更を加えることにより、チケット発行の場合とチケット譲渡の場合とで、(受信側)制御部230における処理が同一化可能となる。

40 【0337】・信頼情報生成部150による信頼情報生成(S1103)の際に、自らのフィンガープリント $H(Pk_I)$ を、発行者による信頼対象 t_1 に含ませる。

【0338】・トークン交換形式 e 生成(S1108)の際に、 $e_7 = Spk_I(Pk_I), e_8 = Pk_I$ とする。

【0339】・トークン交換形式 e の検証(S1111)の際に、式(1)-(4)のかわりに式(8-14)を用いる。(ただし、 U_b は U に置き換える)

(8-2) 利用者装置によるチケット発行

下記の通り、利用者装置に、自己を発行者とするトークン(のみ)を生成する機能を持たせることにより、利用

者装置によるチケット発行が可能になる。

【0340】また、以下の手順により、利用者装置200によるチケット発行を行なうことが可能になる。ただし、以下の説明においてはデータmは生成済であるとする。

【0341】・制御部210は、チケットに対応するデータのハッシュ値 $H(m)$ と、信任対象の $t_1=\{H(PkA_1), H(PkA_2), \dots, H(PkA_i)\}$ を制御部230に与える。

【0342】・制御部230は、保持する検証鍵 PkU を用い、格納部270に $(H(m), H(PkU))$ を格納する。

【0343】・制御部230は、署名部250を用いて $t_2=SpkU(H(PkA_1) \parallel H(PkA_2) \parallel \dots \parallel H(PkA_i))$ を生成する。

【0344】・制御部230は、 $(t_1, t_2, t_3=PkU)$ を制御部210に返却する。

【0345】制御部210は (t_1, t_2, t_3) を格納部220に格納する。以下、チケット譲渡を行なう。

【0346】なお、上記の還流、回数券、再送制御、発行のバリエーションの例は、第1の実施例にも適用可能である。

【0347】また、上記の実施例は、図13～図16に示す構成に基づいて説明したが、この例に限定されことなく、発行者装置、利用者装置、改札者装置、及び接続装置の各機能をプログラムとして構築し、発行者装置、利用者装置、改札者装置、及び接続装置として利用されるコンピュータに接続されるディスク装置や、フロッピーディスク、CD-ROM等の可搬記憶媒体に格納しておき、本発明を実施する際にインストールすることにより、容易に本発明を実現できる。

【0348】図21は、本発明の実施例で説明した記録媒体を使用するコンピュータシステムのハードウェア構成の例を示すブロック図である。本コンピュータシステムは、処理を実行するCPU500、プログラムやデータを記憶するメモリ501、メモリ501またはCPU500で使用するプログラムやデータを蓄積する外部記憶装置502、データを表示するディスプレイ503、データまたは命令を入力するキーボード504、ネットワークを介して他のコンピュータシステム等と通信を行うための通信処理装置505から構成される。上記プログラムはメモリ501又は外部記憶装置502にインストールされCPU500により実行される。

【0349】なお、本発明は、上記の実施例に限定されことなく、特許請求の範囲内において、種々変更・応用が可能である。

【0350】

【発明の効果】上述のように、本発明によれば、発行者が信用する経路のみを介してトークンを移送し、利用者や改札者が当該発行者を特定することにより、データに対応するトークンについて、該トークン内のトークン発行者情報が示す発行者以外により、該トークンをトークン格納部に新規に格納することを防止すると共に、該ト

ークンが転送の過程において複数のトークン格納部に複製されることを防止する。

【0351】また、トークンを原本情報とし、特定の発行者により発行されたトークンを伴うデータのみを原本とすることにより、当該発行者が原本数を制限することが可能となる。

【0352】また、ネットワーク上に存在する情報の識別子(URLなど)をデータとして用いることにより、該情報の複製不能かつ譲渡可能なアクセス権を実現することができる。

【0353】また、権利内容を記述したチケットないし、当該チケットの識別子を本発明におけるデータとして用い、有効なトークンを伴うチケットのみを有効なチケットとし、利用者や改札者がそれ以外を無効なチケットとして拒否することにより、チケット自体を耐タンパ装置に格納することなしに、チケットの不正な行使(二重使用や不当な複製など)を防止することが可能となる。

【0354】また、プログラムを本発明におけるデータとして用い、特定の発行者により発行されたトークンを該プログラムの実行ライセンスとし、プログラムの実行器は、該トークンを伴うプログラム以外の実行を拒否することにより、不当に複製された該プログラムの実行を防止することが可能となる。

【0355】また、音楽データや画像データを本発明におけるデータとして用い、特定の発行者により発行されたトークンを該データの鑑賞権として用い、データの表示器もしくは、再生器は該トークンを伴うデータ以外の表示や再生を拒否することにより、不当に複製された該データの鑑賞を防止することができる。

【図面の簡単な説明】

【図1】本発明の第1の実施例における原理を説明するための図である。

【図2】本発明の第1の実施例のデータ蓄積システムの全体構成図である。

【図3】本発明の第1の実施例のデータ蓄積システムの発行者装置の構成図である。

【図4】本発明の第1の実施例のデータ蓄積システムの利用者装置の構成図である。

【図5】本発明の第1の実施例のデータ蓄積システムの改札者装置の構成図である。

【図6】本発明の第1の実施例のデータ蓄積システムの接続装置の構成図である。

【図7】本発明の第1の実施例のデータ蓄積システムのチケット発行処理のシーケンスチャートである。

【図8】本発明の第1の実施例のデータ蓄積システムのチケット譲渡処理のシーケンスチャート(その1)である。

【図9】本発明の第1の実施例のデータ蓄積システムのチケット譲渡処理のシーケンスチャート(その2)で

ある。

【図10】本発明の第1の実施例のデータ蓄積システムのチケット消費処理のシーケンスチャートである。

【図11】本発明の第2の実施例の原理構成図である。

【図12】本発明の第2の実施例の原本流通システムにおけるデータ蓄積システムの構成図である。

【図13】本発明の第2の実施例の原本データ流通システムの発行者装置の構成図である。

【図14】本発明の第2の実施例の原本データ流通システムの利用者装置の構成図である。

【図15】本発明の第2の実施例の原本データ流通システムの改札者装置の構成図である。

【図16】本発明の第2の実施例の原本データ流通システムの接続装置の構成図である。

【図17】本発明の第2の実施例の原本データ流通システムのチケット発行の場合の動作を示すシーケンスチャートである。

【図18】本発明の第2の実施例の原本データ流通システムのチケット譲渡の場合の動作を示すシーケンスチャート（その1）である。

【図19】本発明の第2の実施例の原本データ流通システムのチケット譲渡の場合の動作を示すシーケンスチャート（その2）である。

【図20】本発明の第2の実施例の原本データ流通システムのチケット消費の場合の動作を示すシーケンスチャートである。

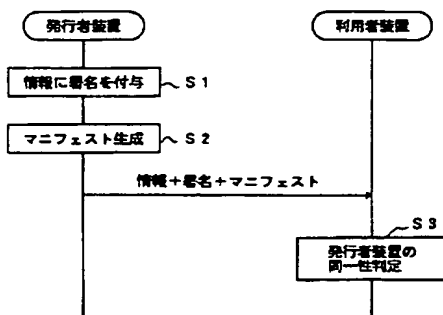
【図21】コンピュータの構成図である。

【符号の説明】

- 1、100 発行者装置
- 2、200 利用者装置
- 3、300 改札者装置
- 4、400 接続装置
- 11、110 制御部
- 12、120 署名部

【図1】

本発明の第1の実施例における原理を説明するための図



13、130 データ生成部

14 マニフェスト生成部

15、150 信任情報生成部

21、210 制御部

22、220 格納部

23、230 制御部

24、240 認証部

25、250 署名部

26、260 番号生成部

10 27、270 格納部

31、310 制御部

32、320 認証部

33、330 番号生成部

34、340 格納部

41、410 通信部

50 発行者装置

51 第1の原本性情報生成手段

52 第1の原本性情報転送手段

60 利用者装置

20 61 第2の原本性情報転送手段

62 第1の特定手段

63 第1の認証手段

64 格納手段

70 改札者装置

71 第2の特定手段

72 第2の認証手段

73 データ処理手段

140 トークン生成部

500 CPU

30 501 メモリ

502 外部記憶装置

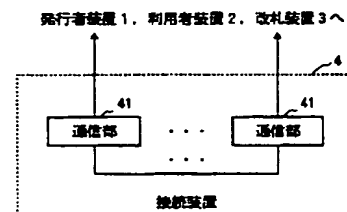
503 ディスプレイ

504 キーボード

505 通信処理装置

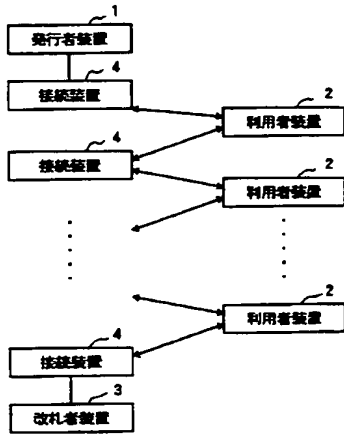
【図6】

本発明の第1の実施例のデータ蓄積システムの接続装置の構成図



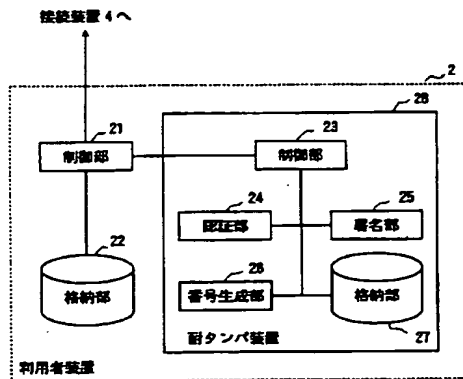
【図2】

本発明の第１の実施例のデータ蓄積システムの全体構成図



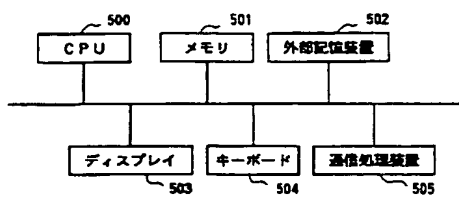
【図4】

本発明の第１の実施例のデータ蓄積システムの 利用者装置の構成図



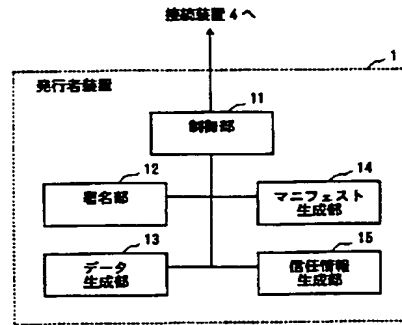
【图 2 1】

コンピュータの構成図



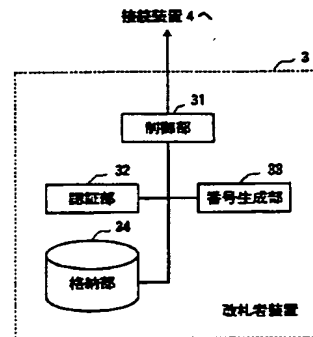
【図3】

**本発明の第１の実施例のデータ蓄積システムの
発行者装置の構成図**



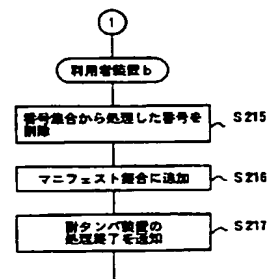
【図5】

本発明の第１の実施例のデータ蓄積システムの改札者装置の構成図

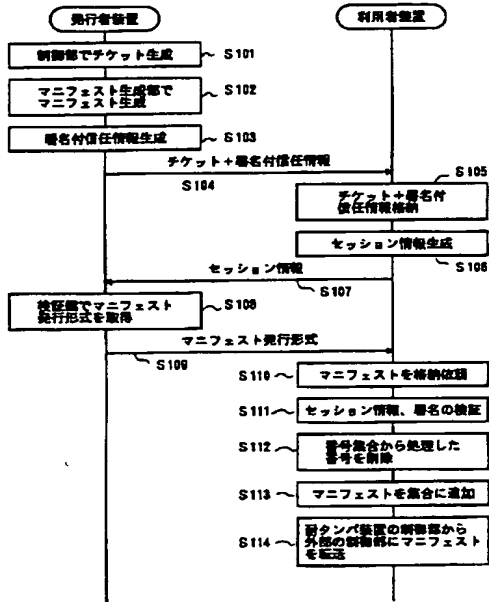


【图9】

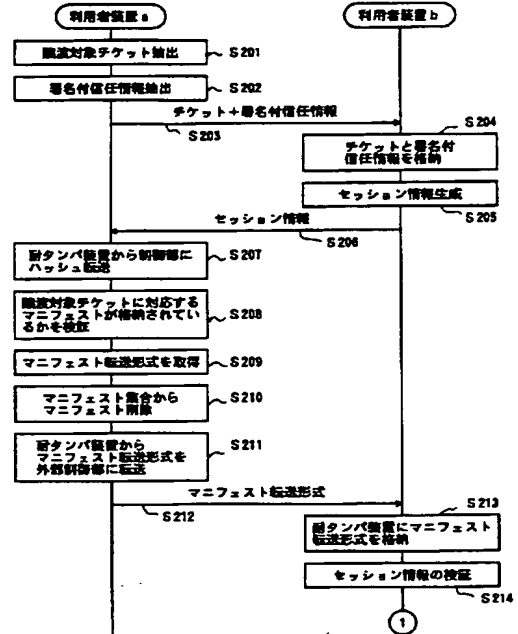
本発明の第１の実施例のデータ蓄積システムの
チケット譲渡処理のシーケンスチャート（その２）



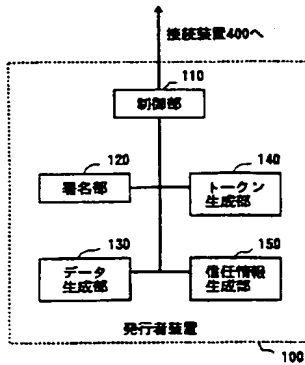
【図7】

本発明の第1の実施例のデータ蓄積システムの
チケット発行処理のシーケンスチャート

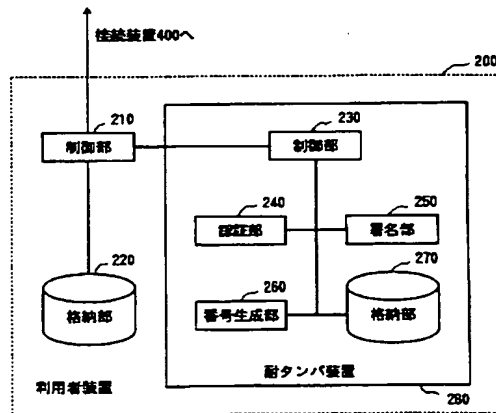
【図8】

本発明の第1の実施例のデータ蓄積システムの
チケット譲渡処理のシーケンスチャート (その1)

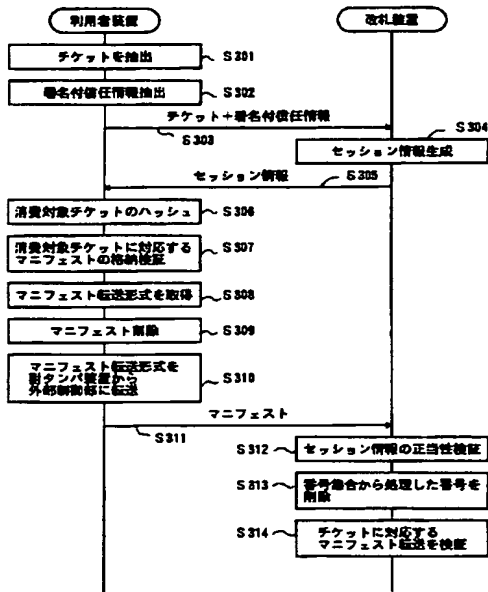
【図13】

本発明の第2の実施例の原本データ流通システムの
発行者装置の構成図

【図14】

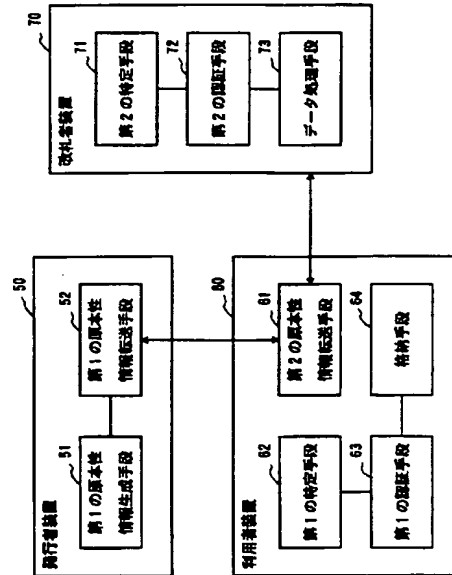
本発明の第2の実施例の原本データ流通システムの
利用者装置の構成図

【図10】

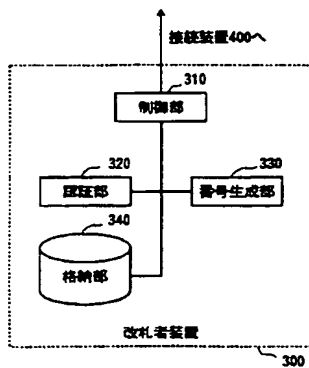
本発明の第1の実施例のデータ蓄積システムの
チケット消費処理のシーケンスチャート

【図11】

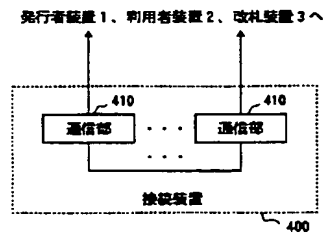
本発明の第2の実施例の原理構成図



【図15】

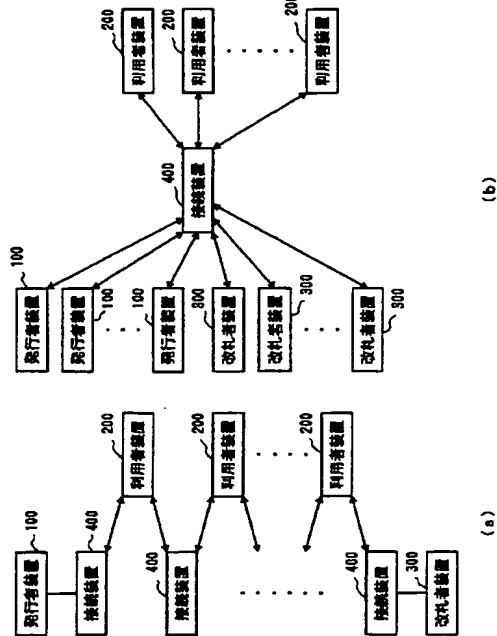
本発明の第2の実施例の原本データ流通システムの
改札者装置の構成図

【図16】

本発明の第2の実施例の原本データ流出システムの
接続装置の構成図

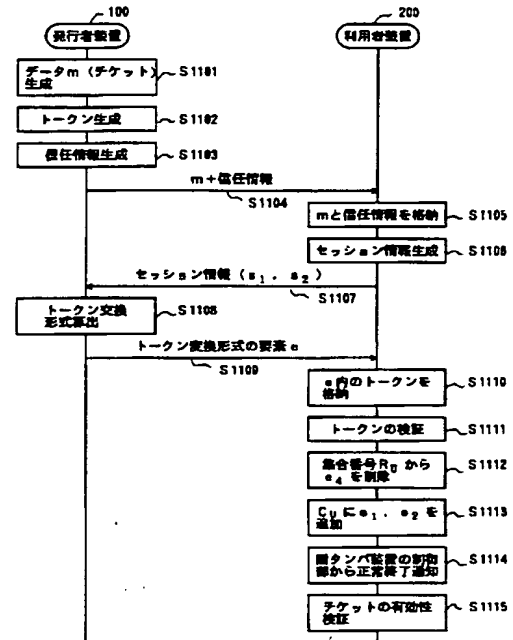
【図12】

本発明の第2の実施例の原本流通システムにおける
データ蓄積システムの構成図



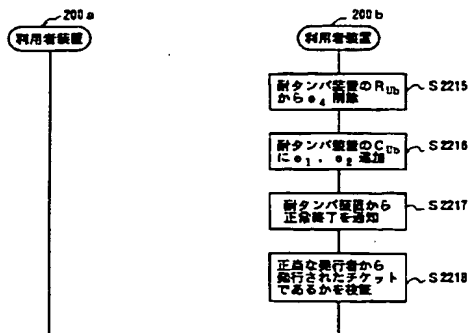
【図17】

本発明の第2の実施例の原本データ流通システムの
チケット発行の場合の動作を示すシーケンスチャート



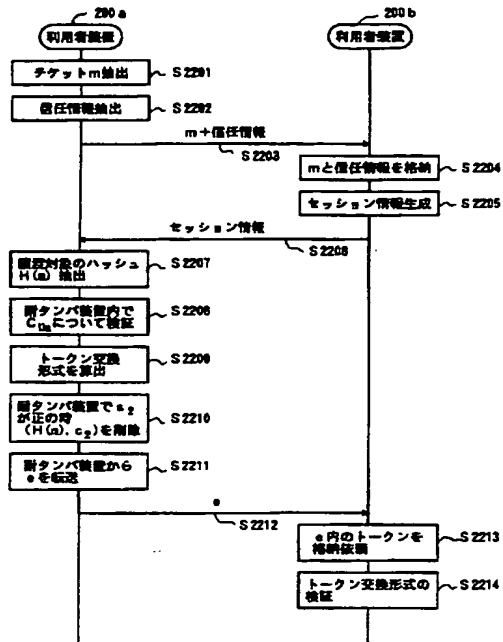
【図19】

本発明の第2の実施例の原本データ流通システムの
チケット譲渡の場合の動作を示すシーケンスチャート(その2)



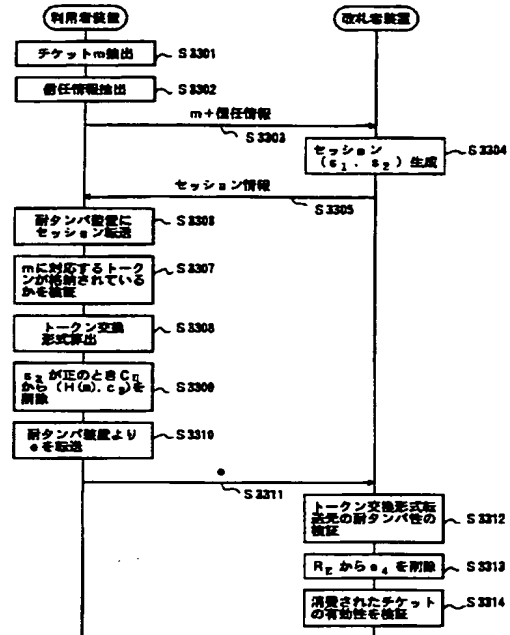
【図18】

本発明の第2の実施例の原本データ流通システムの
チケット譲渡の場合の動作を示すシーケンスチャート (その1)



【図20】

本発明の第2の実施例の原本データ流通システムの
チケット消費の場合の動作を示すシーケンスチャート



フロントページの続き

(51)Int.Cl.⁷

識別記号

F I

テーマコード (参考)

H 0 4 L 9/00

6 2 1 A

(72)発明者 久野 浩

東京都千代田区大手町二丁目3番1号 日
本電信電話株式会社内

(72)発明者 花館 蔵之

東京都千代田区大手町二丁目3番1号 日
本電信電話株式会社内

Fターム(参考) 5B017 AA06 BA07 BB02 BB10 CA15

CA16

5B055 BB10 HA02 HA12 HA17 JJ05

KK05

5D044 DE17 DE49 DE50 HL11

5J104 AA09 LA02 LA03 LA06 NA02

NA27 NA42 PA14

9A001 EE03 EE07 JJ51 LL03